Die Prüfdienste des Bundes
und der Länder informieren

Leitfaden

Elektronische Kommunikation und Langzeitspeicherung elektronischer Daten

Version 5.0
Stand: 23.08.2018

Versionsdokumentation				
Version:	Datum:	Kap./Seite:	Grund d. Änderung:	Bearbeiter:
4.0	Oktober 2014	Alle	Einarbeitung EGovG, Neustrukturierung gesamtes Dokument (aus Version 3.5).	AK Signatur
4.1	April 2016	Alle	Einarbeitung 5. SGB-IV-ÄndG, Anforderungen „Online-Geschäftsstelle“, Anforderungen Apps	AK E-Kommunikation
5.0	September 2018 / Mai 2019	Alle	Neustrukturierung und Aktualisierung	AK E-Kommunikation

Herausgeber:

ADV-Arbeitsgemeinschaft
Geschäftsstelle im Ministerium für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen
Fürstenwall 25
40219 Düsseldorf

Tel.: (0211) 855-5
E-Mail: advag@mags.nrw.de

Bundesversicherungsamt
Abteilung 6

Friedrich-Ebert-Allee 38
53113 Bonn
Tel.: (0228) 619-0

Ansprechpartner:

- Prüfgruppe IT des Referates 614
  (Außenstelle Cloppenburg)
  Tel.: (04471) 1807-0
  E-Mail: Referat_614-IT@bvamt.bund.de

- Referat 611
  Tel.: (0228) 619-2611
  E-Mail: Referat_611@bvamt.bund.de

Inhalt:

0 Einleitung und Anwendungshinweise

Im Zeitalter der Digitalisierung unserer Gesellschaft gewinnt die elektronische Kommunikation zunehmend an Bedeutung. In diesem Zusammenhang stellt sich – auch im Bereich der Sozialversicherung - vielfach die Frage nach der Rechtsverbindlichkeit der elektronischen Kommunikation, der Vorgangsbearbeitung und der Langzeitspeicherung elektronischer Daten. Ziel dieses Leitfadens ist es daher, die gesetzlichen Vorgaben zu dieser Thematik zusammenzutragen und die hieraus abgeleiteten Anforderungen der Prüfdienste für die praktische Umsetzung zu formulieren. Dieser Leitfaden ersetzt aber nicht die individuellen Risikoanalysen und das strukturierte Vorgehen bei der Auswahl, Einführung und (gesetzesmäßigen) Umsetzung konkreter Maßnahmen.

Diese steigende Bedeutung in der Praxis wird begleitet von rechtlichen Entwicklungen auf europäischer und nationaler Ebene.
Daher ist es aus Sicht der Prüfdienste erforderlich, den zuletzt 2016 in der Version 4.1 veröffentlichten Leitfaden weiterzuentwickeln und die sich in der Beratungspraxis ergebenden Fragestellungen einzubeziehen.
Neben inhaltlichen Anpassungen wurde in dieser Version auch der Aufbau des Leitfadens geändert. Ziel ist, durch diese Änderung den Leitfaden stärker nach Themenfeldern zu strukturieren und „handhabbarer“ zu gestalten. Daher folgt der Leitfaden folgendem Aufbau:

- Allgemeine Anforderungen an die Gestaltung von Verfahren werden „vor die Klammer gezogen“ und in Abschnitt 1 dargestellt.
- Besondere Anforderungen / Empfehlungen für einzelne Bereiche der elektronischen Kommunikation, Digitalisierung und Speicherung ergeben sich aus den weiteren Abschnitten.

Dieser Leitfaden beinhaltet folgende Abschnitte:

1 Planung / Vorgehen / Gestaltung der Verfahren
2 Datenschutz
3 Übertragung von Papierunterlagen in die elektronische Form
4 Elektronische Kommunikation zwischen SV-Trägern und Versicherten
5 Automatisierte Sachbearbeitung
6 Elektronischer Datenaustausch
7 Langzeitspeicherung und Löschung elektronisch erzeugter Dokumente und Daten

Neben den durch Gesetze und Verordnungen festgelegten Rahmenbedingungen sind insbesondere folgende, vom Bundesamt für Sicherheit in der Informationstechnik (BSI), des Bundesbeauftragten für den Datenschutz und Informationsfreiheit (BfDI) und vom Bundesinnenministerium herausgegebenen Werke, Standards und Empfehlungen in den jeweils aktuellen Fassungen zu beachten:

- Datenschutzgrundverordnung (DS-GVO)
- BSI-Standards 200-1 bis 200-3 und 100-4
- IT-Grundschutzkompendium
- Technische Richtlinie TR-03138 „Ersetzendes Scannen“ (TR-RESISCAN)
- Technische Richtlinie TR-03125 „Beweiswerterhaltung kryptografisch signierter Dokumente“ (TR-ESOR)
- Technische Richtlinie TR-03147 „Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen“

- „Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“ (BfDI vom 01.03.2013)
- „Minikommentar zum Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften“ (BMI Referat O2 – Stand: 27.06.2013)[1]
- Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informations- und Kommunikationstechnik – Leitlinien und gemeinsame Maßstäbe für IuK-Prüfungen, Stand: November 2011
- Organisationskonzept elektronische Verwaltungsarbeit (Herausgeber: Bundesministerium des Innern)
- Mindeststandard des BSI für den Einsatz des SSL / TLS-Protokolls durch Bundesbehörden (Version 1.0, Stand 2014)
- Richtlinie des GKV-Spitzenverbandes zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Abs. 4b SGB V

Der Leitfaden verweist an den entsprechenden Stellen hierauf.

Dieser wird von den Prüfdiensten des Bundes und der Länder laufend gepflegt und weiter entwickelt. Er wird bei Prüfungen als Grundlage für die Beurteilung dieser Verfahren angewendet.

Den der Prüfung nach § 274 SGB V unterliegenden Institutionen wird empfohlen, ihre Verfahren entsprechend den Ausführungen in diesem Leitfaden zu gestalten. Die Institutionen werden im Text unter dem Begriff „**SV-Träger**“[2] zusammengefasst.

Bei der Einführung von Verfahren der elektronischen Kommunikation handelt es sich um „grundlegende Maßnahmen“ im DV-Bereich. Diese sind rechtzeitig vor der Anschaffung bzw. vor Abschluss verbindlicher Vereinbarungen der Aufsicht unter Verwendung des „Grundleitfaden 85“ (Grundleitfaden für Anzeigen zur Beschaffung bzw. Entwicklung von Datenverarbeitungsanlagen und -systemen sowie -programmen nach § 85 Abs. 1 Sätze 2 – 6 SGB IV, in der Fassung vom 25. November 2008)[3] anzuzeigen.

Bei einer Aufgabenwahrnehmung durch Dritte (§ 197b SGB V) wird empfohlen, die den bundesunmittelbaren Krankenkassen mit Rundschreiben vom 14. Mai 2012 (Az.: II5-5422.0-5272/2011) übermittelten Grundsätze „Anforderungskatalog Outsourcing“ [4] zu beachten.

Es wird darauf hingewiesen, dass zur Vereinfachung der Lesbarkeit auf ein Gendering verzichtet wurde.

---

[1] Abrufbar unter: https://www.verwaltung-innovativ.de/SharedDocs/Publikationen/Artikel/Minikommenta_EGov_Gesetz.pdf

[2] **SV-Träger** i.S.v. § 274 SGB V: Krankenkassen, Pflegekassen, Arbeitsgemeinschaften, Landesverbände der Krankenkassen, GKV-Spitzenverband, Kassenärztliche Bundesvereinigung (KBV),Kassenzahnärztliche Bundesvereinigung (KZBV), Kassenärztliche Vereinigungen (KVs), Kassenzahnärztliche Vereinigungen (KZVs), Medizinischer Dienst des Spitzenverbandes Bund der Krankenkassen (MDS) Medizinische Dienste der Krankenversicherung (MDKs).

[3] Abrufbar unter: http://www.bundesversicherungsamt.de

[4] Abrufbar unter: http://www.bundesversicherungsamt.de. Die Anforderungen werden derzeit durch die Aufsichtsbehörden des Bundes und der Länder überarbeitet; diese ggf. neuen Anforderungen werden in der nächsten Version des Leitfadens aufgegriffen.

1 Planung / Vorgehen / Gestaltung der Verfahren

1.1 Einleitung

Der Abschnitt „Planung / Vorgehen / Gestaltung der Verfahren“ bietet einen Überblick wichtiger Analysen, Maßnahmen und Rahmenbedingungen, die bei der Einführung oder Änderung von Verfahren aus dem Bereich der elektronischen Kommunikation durchzuführen oder zu beachten sind. Dabei ist es unerheblich, ob es sich lediglich um die Überarbeitung eines abgegrenzten, digitalen Informationsangebotes, die Entwicklung bzw. Erweiterung einer Online-Geschäftsstelle oder gar die Einführung eines Verfahrens zur automatisierten Sachbearbeitung handelt. Abhängig von Art, Umfang und Komplexität des Verfahrens kann die Durchführung einiger Schritte bzgl. des Detaillierungsgrades variieren. Alle nachfolgend genannten Schritte tragen aus Sicht der Prüfdienste des Bundes und der Länder zum Projekterfolg und der Reduzierung von Risiken bei.

Bei den Schritten handelt es sich um:

- Erstellung eines Projektvorschlages / Projektanbahnung
- Vorbereitende Analysen und Maßnahmen
  - Geschäftsprozessanalyse und -optimierung
  - Datenschutzrechtliche Anforderungen an Gestaltung von Verfahren
  - Berücksichtigung von Art. 25 DS-GVO (Datenschutz durch Technik)
  - Berücksichtigung von Art. 32 DS-GVO (Sicherheit der Verarbeitung)
  - Datenschutzfolgenabschätzung
  - Einrichtung eines Meldewesens bei Datenschutzverletzungen
- Begleitende und nachgehende Betrachtung
  - Zielerreichung
  - Wirtschaftlichkeitsbetrachtung
  - Bewertung Risikomanagement / Compliance
  - Anzeigen an Aufsichtsbehörden
  - IT-Sicherheit / Datensicherheit
  - Risikomanagement / Compliance / Interne Kontrollsysteme
  - Change Management

Ein Geschäftsprozessanalyse und ggf. -optimierung, Analysen und Festlegungen zu Datenschutz und Datensicherheit, Wirtschaftlichkeitsbetrachtungen sowie – falls keine ausdrücklichen Ausnahmetatbestände vorliegen – die Anzeige an die Aufsichtsbehörde sind aus Sicht der Prüfdienst zwingend durchzuführen.

Da Änderungen oder Neueinführungen von Verfahren in Organisationen meist keine einmaligen Vorgänge sind, sollten die dabei durchzuführenden Schritte in einem **Vorgehensmodell** festgelegt sein. Ein solches Vorgehensmodell geht über die in diesem Abschnitt des Leitfadens dargestellten Punkte hinaus, da es auch wesentliche Rollen und deren Aufgaben, Meilensteine, Entscheidungspunkte sowie weitere Maßnahmen, Produkte und Dokumente beschreibt. Beispiele für sehr umfassende allgemeine Vorgehensmodelle sind das V-Modell XT oder der Rational Unified Process; solche allgemeinen Modelle lassen sich häufig auf die jeweilige Organisation und Projektsituation zuschneiden (sog. Tailoring) oder können bei der Erstellung eines organisationsspezifischen Vorgehensmodells als Orientierung dienen.

1.2 Projektanbahnung

Zur Vorbereitung der Entscheidung, ob ein Projekt umgesetzt werden soll, sollte zunächst die aktuelle Situation im betroffenen Bereich betrachtet werden. Bei Änderungen oder der Ablösung bestehender Verfahren bzw. Prozesse sollten bestehende Prozessabläufe dargestellt und die

wichtigsten Kennzahlen erhoben werden. In diesem frühen Stadium genügt eine grobe Darstellung der Prozessabläufe – eine detaillierte Geschäftsprozessanalyse erfolgt erst später im Projektverlauf. Weiterhin müssen die wesentlichen organisatorischen, technischen und rechtlichen Rahmenbedingungen identifiziert und beschrieben werden.

Durch die **Betrachtung der Ausgangslage** können ggf. vorhandene Schwächen ermittelt und bewertet werden. Sollten keine erheblichen Schwachstellen zu finden sein und auch keine rechtlichen Vorgaben eine Änderung erforderlich machen, so ist bereits an dieser Stelle zu hinterfragen, ob das Projekt überhaupt durchgeführt werden muss.

Wurden Schwächen identifiziert, so stellt deren Behebung den Ausgangspunkt für die Formulierung konkreter **Projektziele** dar. Weitere Ansätze für die Projektziele können die Gesamtstrategie der Organisation oder deren IT-Strategie sowie die Erfüllung neuer rechtlicher Vorgaben liefern. Grundsätzlich gilt, dass nicht das neue Verfahren die Ziele definieren sollte, sondern umgekehrt – anders ausgedrückt: es sollte nicht erst das Softwareprodukt ausgesucht werden und dann die Einsatzmöglichkeit.

Die Projektziele sollten so festgelegt und formuliert sein, dass deren Erreichung später überprüft werden kann. Auch die Buchung der Kosten eines Projekts ist abhängig von dessen Zielen. Liegt die Zielsetzung eines Projektes im Bereich gesundheitliche Aufklärung oder auch Mitgliederwerbung, so sind die Kosten auch dann auf den entsprechenden Konten zu verbuchen, wenn für die Umsetzung des Projektes informationstechnische Lösungen verwendet werden.

Unabhängig davon, ob die Projektziele aus der Gesamt- oder der IT-Strategie hergeleitet wurden, sich aus Schwächen der bisherigen Prozesse oder aus rechtlichen Anforderungen ergeben, sollte immer ein Abgleich mit den strategischen Zielen und Vorgaben vorgenommen werden. Einerseits sollte die Einführung oder Änderung eines Verfahrens zum Erreichen der strategischen Ziele beitragen, andererseits enthalten die übergeordneten Leitlinien Vorgaben, die berücksichtigt werden müssen. Eine Ausrichtung an der **Gesamt- und IT-Strategie** verringert auch das Risiko der Entstehung von Insellösungen, die sich schlecht in die bestehenden oder zukünftigen organisatorische und technische Strukturen einfügen.

Spätestens der Abgleich mit den Vorgaben aus den übergeordneten Leitlinien erfordert eine grobe Vorstellung bzgl. der organisatorischen und technischen Umsetzung des einzuführenden oder zu ändernden Verfahrens. Auch wenn die Ausgestaltung in dieser Phase i.d.R. noch nicht endgültig bekannt sein dürfte, sollte eine **allgemeine Verfahrensbeschreibung** erstellt werden. Davon ausgehend kann eine erste Abschätzung der zu erwartenden **Risiken** sowie der **Wirtschaftlichkeit** vorgenommen werden. Eine detaillierte Risikoanalyse sowie Wirtschaftlichkeitsbetrachtungen sind erst in den folgenden Projektphasen vorzunehmen.

Schon in dieser frühen Phase sollte auch geprüft werden, ob **Wechselwirkungen** mit anderen Verfahren oder Geschäftsprozessen bestehen oder möglich sind. Andere betroffene Fachbereiche des SV-Trägers können so rechtzeitig informiert und beteiligt werden. Auf diese Weise können gegenläufige Entwicklungen vermieden und möglicherweise Synergieeffekte genutzt werden. Im weiteren Projektverlauf wird dieser Punkt insbesondere im Zusammenhang mit Querschnitts- bzw. Basisfunktionen, Schnittstellen und Standards relevant.

Die Ergebnisse der oben beschriebenen Schritte sollten in Form eines **Projektvorschlages** festgehalten werden. Auf dieser Basis ist von den entsprechenden Stellen zu entscheiden, ob das Projekt begonnen werden soll; ob eine ggf. vorgestellte Lösung umgesetzt wird, kann zu diesem Zeitpunkt noch nicht entschieden werden, da hierfür im Projekt erst die Entscheidungsgrundlagen erarbeitet werden müssen.

Wurde beschlossen, dass ein Projekt begonnen werden soll, so müssen anfangs zahlreiche allgemeine Aufgaben des Projektmanagements durchgeführt werden. Beispielsweise sollte ein Lenkungsausschuss gebildet, eine Projektleitung ernannt, ein Projektplan erstellt sowie die er-

forderlichen personellen, materiellen und finanziellen Ressourcen angemeldet und gesichert werden.

1.3 Vorbereitende Analysen und Maßnahmen

1.3.1 Geschäftsprozessanalyse und -optimierung

In den allermeisten Fällen stehen elektronische Verfahren nicht für sich, sondern dienen vornehmlich dem Ziel, **Geschäftsprozesse zu unterstützen**. Sind die entsprechenden Prozesse nicht bereits in einem Prozesshandbuch beschrieben, so stellt die Analyse und Dokumentation bestehender bzw. die Konzeption neu einzuführender Geschäftsprozesse einen der wesentlichen Schritte bei der Einführung von Verfahren der elektronischen Kommunikation dar. Hieraus resultiert auch, dass es sich bei Projekten zur Einführung solcher Verfahren regelmäßig um Organisationsprojekte (auch mit fachlichen Fragen) und weniger um rein technische Projekte handelt.

In vielen Fällen bietet die Einführung elektronischer Verfahren neue Möglichkeiten zur Gestaltung der Prozesse (z. B. Parallelisierung oder Automatisierung). Von daher ist insbesondere bei bestehenden Geschäftsprozessen eine **Analyse und Optimierung** der Prozesse unter Berücksichtigung der ggf. neuen Möglichkeiten geboten. Dabei sollte der einzelne Geschäftsprozess nicht isoliert betrachtet werden, sondern immer im Zusammenhang mit seinen Vorgänger- und Nachfolgeprozessen, so dass Medienbrüche zwischen den Prozessen bzw. die Schaffung von „Insellösungen“ vermieden werden können – ggf. durch Erweiterung des Einsatzbereichs des einzuführenden Verfahrens oder die Schaffung von Schnittstellen.

Neben den direkten Vorgänger- und Folgeprozessen sollten auch Wechselwirkungen mit weiteren Prozessen betrachtet werden. Abgesehen von ggf. ähnlich gestalteten Prozessen im selben oder in anderen Teilen der Organisation sind dabei auch die Wechselwirkungen zwischen **Kern-, Management- und Unterstützungsprozessen** zu berücksichtigen. Falls in der Organisation bereits eine Prozesslandkarte existiert, kann diese hierfür wichtige Anhaltspunkte bieten.

Bei der (Um-)gestaltung von Prozessen sind neben den fachlichen und technischen Anforderungen und den rechtlichen Rahmenbedingungen auch die **organisationsweite Strategie sowie die IT-Strategie** zu berücksichtigen.

Für die strukturierte Darstellung von Geschäftsprozessen haben sich verschiedene grafische oder auch tabellarische **Prozessmodelle** etabliert. Einen Überblick bietet das Organisationshandbuch des Bundesverwaltungsamtes[5]. Innerhalb einer Organisation ist es in der Regel empfehlenswert, sich für eines dieser Modelle zu entscheiden und dieses möglichst organisationsweit zu verwenden. Hat sich das Prozessmodell in der Organisation etabliert, so erleichtert dies nicht nur die Dokumentation selbst sondern vor allem auch den Umgang mit den Ergebnissen.

Trotz gründlicher Analyse und Konzeption kann sich im **Wirk-** / **Produktivbetrieb** zeigen, dass die neuen Prozesse nicht die an sie gestellten Erwartungen erfüllen oder die Prozesse nicht korrekt umgesetzt werden. Aus diesem Grund sollten die Prozesse nach einer gewissen Anlaufphase nochmals kritisch betrachtet und ggf. angepasst werden.

[5] Abrufbar unter: https://www.verwaltunginnovativ.de/OHB/DE/Organisationshandbuch/6_MethodenTechniken/62_Dokumentationstechniken/624_Prozessmodelle/prozessmodelle-node.html

1.3.2 Datenschutzrechtliche Anforderungen an Gestaltung von Verfahren

Bei der Gestaltung neuer bzw. der Änderung bestehender Verfahren sind insbesondere durch die DS-GVO neue Anforderungen entstanden. Diese sind bereits frühzeitig in der Planung und Entwicklung zu berücksichtigen[6].

Dabei handelt es sich nicht allein um technische Anforderungen, die bei der Programmierung etc. zu beachten sind, sondern auch um Fragen der Verfahrensgestaltung. Daher sind auch bei der Entwicklung frühzeitig die Bereiche IT, übergreifende Bereiche (Organisation, Datenschutz etc.) sowie die Fachbereiche einzubeziehen.
Die entsprechenden Abwägungen zur Wahl der Maßnahmen und Ausgestaltung der Verfahren sollten frühzeitig erfolgen und auch nachvollziehbar dokumentiert werden.

1.3.2.1 Art. 25 DS-GVO

Art. 25 DS-GVO verpflichtet die Verantwortlichen in seinen Absätzen 1 und 2 zu folgenden Punkten:

- Datenschutz durch Technik – „data protection by design“
  Die Verantwortlichen werden dabei verpflichtet, geeignete technische und organisatorische Maßnahmen umzusetzen.
  Im Rahmen der Erörterung von entsprechenden Maßnahmen (z. B. Pseudonymisierung) sollte eine vorgenommene Abwägung und objektive Bewertung von Umständen wie dem Stand der Technik, Implementierungskosten und auch Risiken für Rechte und Freiheiten der Betroffenen dokumentiert werden.
- Datenschutz durch Voreinstellung – „data protection by default“
  Die Verantwortlichen werden verpflichtet, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass durch Voreinstellungen im technischen Verfahren grundsätzlich nur die personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind.[7]
  Dabei gilt die Verpflichtung, die Voreinstellungen entsprechend auszurichten, für die Frage der Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.[8]
  Im Rahmen der Erörterung von entsprechenden Maßnahmen sollten auch an dieser Stelle vorgenommene Diskussionen und Abwägungen dokumentiert werden.

1.3.2.2 Art. 32 DS-GVO

Art. 32 DS-GVO regelt – als Querschnittsthema - die Sicherheit der Verarbeitung personenbezogener Daten und damit, wer welche technischen und organisatorischen Maßnahmen treffen muss, um ein angemessenes Schutzniveau bei der Verarbeitung sicherzustellen.
Dabei ist zur Bestimmung der geeigneten und angemessenen Maßnahmen abzuwägen (Verhältnismäßigkeit):

---

[6] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder „Standard Datenschutzmodell: Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele“ (Version 1.1).

[7] BeckOK DatenSR/Paulus DS-GVO Art. 25 Rn. 8.

[8] BeckOK DatenSR/Paulus DS-GVO Art. 25 Rn.10.

- Stand der Technik (das technisch Mögliche und Erprobte; hier ist das europarechtliche Begriffsverständnis zu Grunde zu legen)
- Kosten
- Art und Weise der Verarbeitung
- mögliche Schäden (Risiken für Rechte und Freiheiten der natürlichen Personen)[9]

Auch diese Erörterungen sind zu dokumentieren.

Die Umsetzung der Erörterungen bzw. technisch-organisatorischen Maßnahmen im Prozess sollten im weiteren Verlauf der Umsetzung festgehalten werden.

1.3.3 Datenschutzfolgenabschätzung

Die entsprechenden Maßnahmen der vorgenannten datenschutzrechtlichen Betrachtungen sind dann im Rahmen einer ggf. erforderlichen Datenschutzfolgenabschätzung einzubringen (siehe Abschnitt Datenschutz)[10].

1.3.4 Einrichtung eines Meldewesens bei Datenschutzverletzungen

Neben den Anforderungen an die Gestaltung von Verfahren sind ggf. auch neue Verfahren an sich zu errichten.

Dabei ist die frühzeitige Ausgestaltung eines trägerinternen und externen Meldeverfahrens bei künftigen Verletzungen des Schutzes personenbezogener Daten bereits im Rahmen der Umsetzungsphase von Vorhaben zu berücksichtigen. Die entsprechenden Bereiche des SV-Trägers (insbesondere Datenschutzbeauftragte) sind vorzugsweise bereits in der Konzeptionsphase einzubinden.

1.4 Begleitende und nachgehende Betrachtung

1.4.1 Zielerreichung

Die in der Vorphase gesetzten Ziele und deren Erreichungsfaktoren sind in der Umsetzungsphase fortzuschreiben und die Zielerreichung an den gesetzten Faktoren zu messen.

Begleitend und im Nachgang der Entwicklung sollten daher Maßnahmen vorgesehen werden, um die Zielerreichung zu messen.

Auf der Grundlage der Zielerreichung sind dann ggf. weitere Maßnahmen zu erörtern. Die Ergebnisse können dazu führen, dass bei der Umsetzung des Verfahrens / Geschäftsprozesses nachzusteuern ist, um die gesetzten Ziele (besser) zu erreichen.

Die Analyse der Zielerreichung kann auch als Erkenntnisquelle für die Weiterentwicklung bzw. die Entwicklung weiterer Prozesse herangezogen werden.

---

[9] Jandt in Kühling / Buchner DS-GVO, Art. 32, ab Rn. 7.

[10] Siehe z. B. Art.29-Gruppe, Working Paper 249, Punkt 9.

Dafür ist dann erforderlich, dass diese Erkenntnisse auch den beteiligten Bereichen bzw. Organisationseinheiten, die mit der Umsetzung weiterer Verfahren befasst sind, zur Verfügung gestellt werden.

Die Messung an den im Vorfeld festgelegten Zielerreichungsfaktoren, die ggf. vorzunehmende Anpassung der laufenden Projekte und die (permanente) Betrachtung und Weiterentwicklung der Prozesse, sollten fester Bestandteil des Aufbaus der Einführungsphase neuer Anwendungen / Prozesse und deren Erfolgskontrolle sein.

1.4.2 Wirtschaftlichkeitsbetrachtung

Vor einer Entscheidung über den Einsatz elektronischer Verfahren ist die Wirtschaftlichkeit des Gesamtverfahrens festzustellen (§§ 69 Abs. 2, 110a Abs. 2 SGB IV, 6 Satz 2 EGovG). Hierfür sind die gängigen Verfahren zur Wirtschaftlichkeitsberechnung[11] (§ 69 Abs. 3 SGB IV) anzuwenden. Einzubeziehen sind auch Fragen zur Nachhaltigkeit und zu den Auswirkungen / Kosten bei einem Systemwechsel. Zu beachten ist hierbei, dass die Erfüllung gesetzlicher Vorgaben – insbesondere aus §§ 110a - c SGB IV sowie SGB X – Vorrang vor dem Gebot des wirtschaftlichen Handelns hat.

Die bereits in der Vorphase anzulegende grundlegende Wirtschaftlichkeitsbetrachtung ist im Verlauf des Umsetzungsverfahrens weiter fortzuschreiben.

Aus der Fortschreibung sollten regelmäßige Berichte mit Entwicklungen / entstehenden Risiken erstellt werden.

Nach Abschluss der Implementierung sollte die abschließende Wirtschaftlichkeitsbetrachtung analysiert werden, um Anhaltspunkte / Annahmen für weitere Verfahren zu erhalten bzw. dort Risiken frühzeitig erkennen zu können.

1.4.3 Informationen zur Bewertung von Risikomanagement / Compliance

Das (bestehende) Risikomanagement des SV-Trägers muss auch die neuen Systeme und Prozesse umfassen.

Daher sind aus dem Umsetzungsprozess bzw. der Entwicklung heraus die entsprechenden Informationen aus dem konkreten Verfahren für das Risikomanagement aufzubereiten und diesem bzw. der hierfür zuständigen Stelle zuzuleiten.
Die identifizierten Risiken (z. B. Datenverlust / Datensicherheit, eingeschränkte Erreichbarkeit, technische Fehler, IT-Sicherheit / Ausfall, Ausschluss fachliche Fehler) sollten monetär wie nicht-monetär bewertet und dokumentiert werden.

Maßnahmen zu deren Bewältigung sind zu entwickeln und auch noch im Wirkbetrieb fortzuschreiben.

Anhaltspunkte für eine derartige Risikoanalyse bietet der BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz.

[11] Band 18 der Schriftenreihe des Bundesbeauftragten für Wirtschaftlichkeit in der Verwaltung BWV (Präsident des Bundesrechnungshofes): „Anforderungen an Wirtschaftlichkeitsuntersuchungen finanzwirksamer Maßnahmen nach § 7 Bundeshaushaltsordnung“.

Auch sollten die neuen Instrumente im Hinblick auf das (bestehende) Compliance-Umfeld der SV-Träger ausgerichtet werden und eine entsprechende Information an die verantwortliche Stelle erfolgen.

1.4.4 Vergabeverfahren

Nach § 22 SVHV muss dem Abschluss von Verträgen über Lieferungen und Leistungen mit Ausnahme der Verträge, die der Erbringung gesetzlicher oder satzungsmäßiger Versicherungsleistungen dienen, eine öffentliche Ausschreibung vorausgehen. Hiervon kann in Ausnahmefällen abgesehen werden, sofern die Natur des Geschäfts oder besondere Umstände dies rechtfertigen. Landesspezifische Regelungen sind ggf. zu beachten.

Hinweis:
Der Beauftragte der Bundesregierung für Informationstechnik (www.cio.bund.de) hat für die Beschaffung von IT-Leistungen für die Bundesverwaltung ergänzende Vertragsbestimmungen (EVB-IT) für den Abschluss von Verträgen mit externen Anbietern erarbeitet. Die Verträge sollen den öffentlichen Auftraggeber davor schützen, durch die allgemeinen Vertragsbedingungen des Anbieters benachteiligt zu werden.

Die Prüfdienste des Bundes und der Länder raten dringend, die Empfehlungen zu beachten. Näheres über die jeweiligen Vertragswerke sind der o.g. Internetseite zu entnehmen.

1.4.5 Anzeige an Aufsichtsbehörden

Vor Einführung des Verfahrens sind die gesetzlich vorgesehenen Meldungen / Anzeigen an die zuständige Aufsichtsbehörde zu übermitteln.

Gem. § 85 Abs. 1 Satz 2 ff SGB IV ist dabei (bereits) die Absicht, sich zur Aufgabenerfüllung an Einrichtungen mit Ausnahme von Arbeitsgemeinschaften im Sinne dieses Gesetzbuches zu beteiligen, sowie die Absicht, Datenverarbeitungsanlagen und -systeme anzukaufen, zu leasen oder anzumieten oder sich an solchen zu beteiligen, der Aufsichtsbehörde vor Abschluss verbindlicher Vereinbarungen anzuzeigen. Dies gilt auch für die Beschaffung von Datenverarbeitungsprogrammen. Nur solange das Systemkonzept der Datenverarbeitung nicht grundlegend verändert wird, ist eine Anzeige nicht erforderlich.
Jede Anzeige hat so umfassend und rechtzeitig zu erfolgen, dass der Aufsichtsbehörde vor Vertragsabschluss ausreichend Zeit zur Prüfung und Beratung des Versicherungsträgers bleibt.

Bei der Einführung von E-Government-Verfahren, elektronischer Vorgangsbearbeitungssysteme oder der elektronischen Langzeitspeicherung handelt es sich in der Regel um grundlegende Maßnahmen im DV-Bereich. Diese sind somit rechtzeitig vor der Anschaffung bzw. vor Abschluss verbindlicher Vereinbarungen der Aufsicht anzuzeigen.

Die Aufsichtsbehörden haben den „Grundleitfaden 85“[12] erstellt. Dieser bildet den Rahmen für die Anzeige und die Wirtschaftlichkeitsbetrachtung und ist demnach zu beachten.
Soweit sich der Versicherungsträger bei der Erfüllung seiner gesetzlich vorgeschriebenen Aufgaben zulässigerweise eines Dritten bedient, kann er mit Genehmigung der Aufsichtsbehörde auch die damit notwendigerweise verbundenen Aufgaben des Rechnungswesens durch diesen

[12] Abrufbar unter: https://www.bundesversicherungsamt.de/fileadmin/redaktion/Datenschutz_Datensicherheit/Grundleitfaden_85.pdf

Dritten wahrnehmen lassen (§ 19 SVRV). Die ausschließliche elektronische Aufbereitung der Rechnungsbelege durch den Dienstleister ist genehmigungsfrei, aber anzeigepflichtig.

1.4.6 IT-Sicherheit / Datensicherheit

Eine auf den bestehenden und beschriebenen Geschäftsprozessen und den ermittelten Risiken basierende Gesamtdarstellung der Informationssicherheit sollte für den Träger aufgebaut und fortgeschrieben werden. Anhaltspunkte bietet hierfür der BSI-Standard 200-1.

Die BSI-KRITIS-Verordnung bestimmt (nach Anpassung mit Inkrafttreten am 30. Juni 2017 – Korb 2[13]) den Anwendungsbereich in der gesetzlichen Sozialversicherung. Diese hiervon betroffenen SV-Träger müssen nach § 8a BSI-Gesetz innerhalb von zwei Jahren die wesentlichen IT-Systeme entsprechend dem Stand der Technik absichern, hierüber regelmäßig geeignete Nachweise erbringen, eine Kontaktstelle benennen und erhebliche IT-Störungen unverzüglich dem BSI melden.

1.4.7 Risikomanagement / Compliance / Interne Kontrollsysteme

Die neuen bzw. geänderten Verfahren / Anwendungen sind durch die hierfür zuständigen Stellen der SV-Träger in das generelle Risikomanagement, die Compliance-Maßnahmen und das Interne Kontrollsystem des SV-Trägers einzubeziehen.

Dabei sind insbesondere folgende Punkte vorzunehmen:

- Aufnahme in Verfahrensübersicht / Verarbeitungsverzeichnis
- Prüfung der Anwendungen / Systeme auf Einhaltung der allgemeinen Vorgaben des Risikomanagements / der Compliance
- Einbezug der Umsetzung / des Wirkbetriebs der Anwendungen / Systeme in Prüfplan der verantwortlichen Stellen.

1.4.8 Change Management

Änderungen von Prozessen bergen vielfältige Risiken. Zum Teil sind es solche, die auch beim (Neu-)Aufbau von Prozessen auftreten. Änderungen bergen aber auch spezifische Risiken, wie z. B. mögliche Eingriffe in laufende Systeme bzw. Migration von Daten, die im Rahmen von Änderungsprozessen und der Umsetzungsplanung angemessen zu berücksichtigen sind.

Daher sollten die Geschäftsprozesse zum Change Management zur Änderung von Prozessen, Anwendungen sowie fachlicher und technischer Parameter allgemein festgelegt werden. In die Änderungsverfahren sollten auch jeweils die verantwortlichen Stellen des SV-Trägers nach einem festen Geschäftsprozess verpflichtend eingebunden werden:

- Fachbereich (materielles Recht und Fachprozesse)
- IT-Bereich
- Datenschutz
- IT-Sicherheit
- Risikomanagement und Internes Kontrollsystem

[13] Abrufbar z. B. unter: http://www.bundesanzeiger.de

- Speicherung und Archivierung

Eine nachvollziehbare Dokumentation des Änderungsprozesses ist dringend zu empfehlen.

2 Datenschutz

2.1 Einleitung

Die EU-Datenschutz-Grundverordnung (DS-GVO) findet seit dem 25.05.2018 in jedem Mitgliedstaat der EU unmittelbar Anwendung (Art. 99 Abs. 2 DS-GVO). Zahlreiche Öffnungsklauseln (insgesamt mehr als 70) ermöglichten es, die DS-GVO durch eigene Gesetzgebung zu konkretisieren (Art. 88 Abs. 1 DS-GVO), zu ergänzen (Art. 37 Abs. 4 S. 1 DS-GVO) oder zu modifizieren (Art. 17 Abs. 3 b DS-GVO). Dabei haben Gesetze nationaler Gesetzgeber zur Ausfüllung des Rahmenrechts der DS-GVO stets die Vorgaben und Grundsätze der DS-GVO zu beachten. So wurde von diesen Handlungsoptionen Gebrauch gemacht und die Neuregelung des BDSG gesetzlich verankert, welches ebenfalls am 25.05.2018 in Kraft getreten ist. Zahlreiche weitere Ausfüllungen der Öffnungsklauseln der DS-GVO finden sich in Spezialgesetzen, wie etwa im SGB X. In der Normenhierarchie steht die DS-GVO ganz oben. Gesetze, die die DS-GVO konkretisieren, ergänzen oder modifizieren, sind vorrangig zu beachten (s. dazu Abb. 1, S. 20).

Nachfolgend gehen die Prüfdienste auf die für den Bereich der elektronischen Kommunikation der SV-Träger wichtigen datenschutzrechtlichen Regelungen näher ein.

Wesentliche Neuerungen bestehen darin, dass die Rechte der Nutzer durch neue Transparenz- und Informationspflichten der datenverarbeitenden Institutionen gestärkt werden. Neu ist auch die Pflicht, elektronische Geräte und Anwendungen datenschutzfreundlich voreinzustellen. Ebenfalls neu eingeführt wird die Pflicht zur Datenschutzfolgenabschätzung. Die DS-GVO erweitert die bereits bekannten Pflichten und erhöht die rechtlichen, betrieblichen und technisch-organisatorischen Anforderungen an den Datenschutz. Außerdem ist neu, dass auch der Auftragsverarbeiter ein „Verzeichnis der Verarbeitungstätigkeiten“ führen muss.

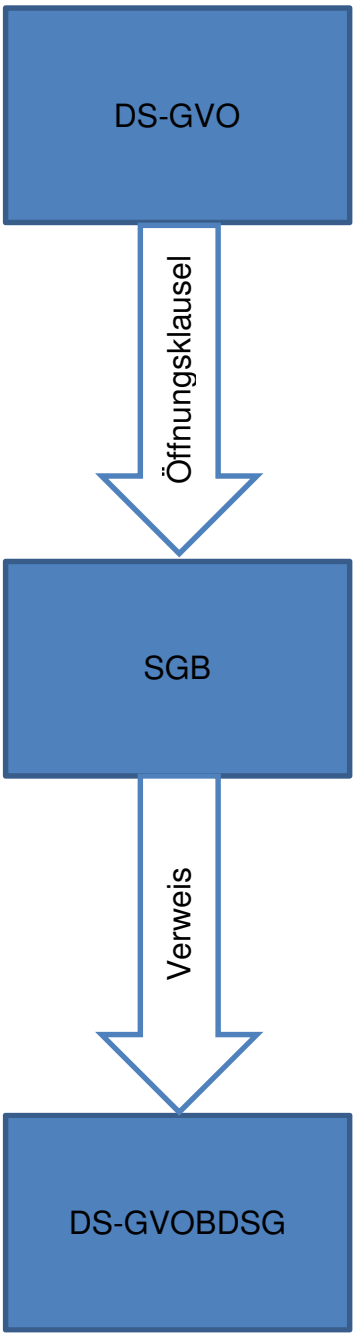
Die Datenschutzbehörden des Bundes und der Länder unterstützen den Prozess und stimmen dazu eine einheitliche Sichtweise ab. Zu diesem Zweck haben sie gemeinsame Kurzpapiere[14] zur DS-GVO herausgegeben, diese dienen als Orientierung, wie die DS-GVO im praktischen Vollzug angewendet werden sollte. Sie stehen unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung durch den Europäischen Datenschutzausschuss.

Auch die Aufsichtsbehörden des Bundes und der Länder im Bereich der Sozialversicherung beschäftigen sich mit entsprechenden, spezifischen Fragen der Umsetzung.[15]

[14] Siehe Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder:
https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/DSGV)_Kurzpapiere.html

[15] Siehe die FAQ des Bundesversicherungsamtes:
https://www.bundesversicherungsamt.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20180522_DSGVO_FAQ_Version_5.pdf

Normenhierarchie zur Anwendung der DS-GVO im Bereich der gesetzlichen Krankenversicherung
gültig ab 25.05.2018



Die DS-GVO gilt unmittelbar

Öffnungsklauseln Art. 6 Abs. 2 und Art. 9 Abs. 2 DS-GVO:
ausgefüllt durch das „Gesetz zu Änderungen zum Bundesversorgungsgesetz und weiterer Gesetze“

SGB I	SGB X
§ 35	§§ 67 - 85a

Dabei Verweis auf BDSG:
Datenschutz-Anpassungs- und -Umsetzungsgesetz EU

Nachfolgende Vorschriften des SGB X verweisen auf Regelungen des BDSG

§ 67a Abs.1
§ 67b
§ 75 Abs. 3, 6
§ 80 Abs. 4
§ 81 Abs. 2, 4
§ 81a Abs. 1
§ 81c
§ 85

Abb. 1

2.2 Regelungen in Spezialgesetzen

Der Bundesgesetzgeber hat die Vorschriften des Ersten Buches Sozialgesetzbuch – Allgemeiner Teil – (SGB I) und des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) an die DS-GVO angepasst. Diese Änderungen sind am 25. Mai 2018 in Kraft getreten.

Die Regelungssystematik des Sozialgeheimnisses in § 35 SGB I sowie der grundsätzlich für jedes Buch des Sozialgesetzbuches geltenden Vorschriften in den §§ 67 ff SGB X wurde redaktionell an die DS-GVO angepasst[16]. Sozialdaten (§ 67 Abs. 1 SGB X) sind personenbezogene Daten (Art. 4 Nr. 1 DS-GVO), die von einer in § 35 SGB I genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Auch werden weiterhin die §§ 67a ff SGB X von dem zentralen Grundsatz bestimmt, dass die Datenverarbeitung nur zulässig ist, wenn die Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle erforderlich ist (Grundsatz der Erforderlichkeit).

Zur Erhebung besonderer Kategorien personenbezogener Daten findet sich keine ausdrückliche gesetzliche Regelung im SGB X. Hier sind die Vorschriften der DS-GVO zu beachten. Die Erhebung auf der Grundlage einer Einwilligung dürfte für öffentliche Stellen angesichts des Erwägungsgrundes 43 DS-GVO nur eine untergeordnete Bedeutung haben.

Nahezu unverändert gilt die Datenübermittlungsvorschrift des § 69 SGB X fort. Dagegen erfolgte eine Ausweitung der Befugnis zur Speicherung, Veränderung, Nutzung und Übermittlung von Sozialdaten für Zwecke der wissenschaftlichen Forschung (§§ 67b Abs. 3, 75 SGB X)

Die Regelung der Rechte der betroffenen Person erfolgt in §§ 81 ff SGB X. Durch die DS-GVO unmittelbar eingeräumte Informationspflichten (Art. 13 DS-GVO), Auskunfts- (Art. 15 DS-GVO), Berichtigungs- bzw. Löschrechte (Art. 16, 17 DS-GVO) sowie das Widerspruchsrecht (Art. 21 DS-GVO) werden dabei in den §§ 82 ff SGB X eingeschränkt.

§ 80 SGB X regelt die Verarbeitung von Sozialdaten im Auftrag. Die Vorschrift entspricht im Wesentlichen dem bisherigen Recht, ist aber redaktionell angepasst worden.

2.3 Rechte der Betroffenen

Die Rechte betroffener Personen (Art. 12 - 23 DS-GVO), deren Daten verarbeitet werden, bringen für Verantwortliche im Sinne des Art. 4 Nr. 7 DS-GVO neue Pflichten mit sich. Die Etablierung eines praktikablen Verfahrens, um DS-GVO-konform auf Ansprüche der Betroffenen reagieren zu können, ist empfehlenswert.

Die Rechte der betroffenen Personen sind grundsätzlich im SGB X geregelt. Diese Rechte sind bei der Gestaltung von Verfahren durch den SV-Träger zu berücksichtigen. Im Einzelnen betrifft dies folgende Rechte:

- Informationspflichten bei der Erhebung von Sozialdaten bei der betroffenen Person gem. § 82 SGB X
- Informationspflichten bei der Erhebung von Sozialdaten nicht bei der betroffenen Person gem. § 82a SGB X

[16] Siehe das “Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften” vom 17. Juli 2017, Bundesgesetzblatt I Seiten 2541 ff.

- Auskunftsrecht der Betroffenen gem. § 83 SGB X
- Recht auf Berichtigung und Löschung gem. § 84 SGB X[17]

2.4 Datenschutzerklärung

Grundsätzlich müssen Institutionen, die Webseitenbetreiber sind, eine Datenschutzerklärung bereithalten. Mit der Datenerhebung muss deutlich werden, welche Daten wie und wozu erhoben werden.

Anforderungen an die Datenschutzerklärung:

- Angabe der Rechtsgrundlage, auf der die Datenverarbeitung beruht (Art. 13 Abs. 1 c)
- Bereithalten aller in Art. 13 genannten, verpflichtenden Informationen
- Formulierung in klarer und einfacher Sprache sowie transparente und verständliche Strukturierung
- Leichte Zugänglichkeit, so dass Betroffene sie mit nur einem Klick erreichen können

2.5 Geeignete technische und organisatorische Maßnahmen (TOM)

Die DS-GVO stellt hohe Anforderungen an die Technik und die interne Organisation des Verantwortlichen. Verantwortliche müssen nach Art. 24, 25 DS-GVO geeignete technische und organisatorische Maßnahmen (TOM) treffen, um die Einhaltung der Datenschutzgrundsätze gem. Art. 5 Abs. 1 DS-GVO, insbesondere die Datenminimierung (Art. 5 Abs. 1 Buchstabe c DS-GVO) und die Datensicherheit (Art. 5 Abs. 1 Buchstabe f DS-GVO) zu gewährleisten, den Vorgaben der DS-GVO zu genügen und die Betroffenenrechte zu schützen (Datenschutz durch Technik, Art. 25 Abs. 1 DS-GVO, auch „privacy by design“ genannt).

Welche Maßnahmen konkret erforderlich sind, hängt u.a. vom Stand der Technik, der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbunden Risiken für die persönlichen Rechte und Freiheiten sowie den jeweiligen Implementierungskosten ab (Art. 25, 32DS-GVO). Dabei müssen die Maßnahmen in einem wirtschaftlich angemessenen Verhältnis zum Schutzbedarf der verarbeiteten personenbezogenen Daten stehen. Es gilt jedoch zu beachten, dass unzureichende Schutzmaßnahmen nicht mit wirtschaftlichen Argumenten gerechtfertigt werden können. Das Gesetz nennt in Art 32 Abs. 1 DS-GVO als wichtige, aber nicht abschließende Vorgaben für Maßnahmen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Hierbei handelt es sich zum einen um IT-Sicherheitskonzepte wie etwa einen geeigneten Virenschutz, eine ausreichende Stromversorgung oder ein Backup-Programm. Auch organisatorische

[17] Zum Verhältnis Berichtigung von Diagnosedaten gem. § 84 SGB X vor dem Hintergrund des Korrekturverbotes gem. § 303 SGB V siehe 92. Arbeitstagung der Aufsichtsbehörden der SV-Träger, TOP 16.

Maßnahmen wie etwa eine wirksame Zutritts-, Zugangs- und Zugriffskontrolle zählen dazu. Zur internen Sicherheit zählen auch Dienstanweisungen an die Beschäftigten – etwa eine Richtlinie zur Kontrolle der Weitergabe von Daten, ein Archivierungs-, Aufbewahrungs- und Löschkonzept, eine Anweisung, wie auf Auskunftsbegehren der Betroffenen zu reagieren ist oder was zu tun ist, wenn ein Notfall eintritt.

Technische Geräte und vor allem IT-Anwendungen müssen zukünftig so voreingestellt werden, dass nur solche Daten erhoben werden, die erforderlich sind, um den jeweiligen bestimmten Verarbeitungszweck zu erreichen (Datenschutz durch datenschutzfreundliche Voreinstellungen, Art. 25 Abs. 2 DS-GVO, auch „privacy by default“ genannt).

Neben der DS-GVO enthält § 67b Abs. 1 Satz 4 SGB X i. V. m. § 22 Abs. 2 BDSG eine konkretere Ausformung der erforderlichen technisch-organisatorischen Maßnahmen[18].

2.6 Datenschutzfolgenabschätzung (DSFA)

Für die Datenschutzfolgenabschätzung (DSFA) gem. Art. 35 DS-GVO müssen Verantwortliche einschätzen, ob die jeweilige Verarbeitung voraussichtlich hohe Risiken für die Rechte oder Freiheiten des Betroffenen ausweist. Sie erfolgt in bis zu drei Stufen und ist schriftlich zu dokumentieren.

1. Eine systematische Risikobewertung (Schwellwertanalyse) ist vorzunehmen. Hier müssen alle einzelnen Prozesse daraufhin überprüft werden, ob im Einzelfall voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlichem Risiko reicht eine gemeinsame Abschätzung (Art. 35 Abs. 1 S. 2 DS-GVO). Ein solches Risiko besteht nach Art. 35 Abs. 3 DS-GVO insbesondere bei der Verwendung neuer Technologien, die automatisiert, systematisch und umfassend Daten erfassen, verarbeiten und bewerten. Auch kann aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein solches Risiko bestehen. Schließlich kann die Verarbeitung besonderer Kategorien von Daten (z. B. Gesundheitsdaten oder Religionszugehörigkeit i.S.d. Art. 9 DS-GVO) eine weitere Prüfung notwendig machen. Als weitere Hilfestellung für die Einschätzung dienen die ersten Leitlinien zur DSFA der Art. 29-Datenschutzgruppe[19]. Die Aufsichtsbehörden gem. Art. 35 Abs. 4 DS-GVO veröffentlichen eine Liste[20] von Verarbeitungsvorgängen, für die eine DSFA verbindlich durchzuführen ist.

2. Wenn ein solches Risiko im Hinblick auf den Prozess besteht, muss in einer zweiten Stufe eine Bewertung dahingehend vorgenommen werden, ob die geplanten Abhilfemaßnahmen und Sicherheitsvorkehrungen ausreichen, um den Schutz der Daten zu gewährleisten. Der Nachweis zur Einhaltung der DS-GVO muss erbracht werden.

3. Verbleibt trotz des Eingreifens technischer und organisatorischer Maßnahmen ein hohes Risiko für die Rechte und Freiheiten der natürlichen Person muss in einer dritten Stufe die Aufsichtsbehörde konsultiert werden (Art. 36 Abs. 1 DS-GVO). Diese kann dann innerhalb von

[18] § 64 Abs. 3 BDSG gilt nicht für SV-Träger, da kein Verweis im SGB enthalten ist. Jedoch können und sollten die Grundgedanken der Norm bei der Gestaltung von Systemen und Verfahren herangezogen werden.

[19] Abrufbar unter: https://www.datenschutz-bayern.de/technik/orient/wp248.pdf

[20] Abrufbar unter: https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/ListeVerarbeitungsvorgaenge.html

acht Wochen Empfehlungen aussprechen (Art. 36 Abs. 2 DS-GVO). Diese Frist kann je nach Komplexität der geplanten Verarbeitung von personenbezogenen Daten von der Aufsichtsbehörde verlängert werden.

Die Datenschutzbeauftragte des SV-Trägers ist beratend in die Durchführung einer DSFA einzubinden (Art. 35 Abs. 2 und Art. 39 Abs. 1 c DS-GVO).

2.7 Melde- und Informationspflichten bei Datenpannen

Nach § 83a SGB X i. V. m. Art. 33 DS-GVO müssen grundsätzlich alle Verletzungen des Schutzes personenbezogener Daten gemeldet[21] werden, es sei denn, das Risiko für persönliche Rechte und Freiheiten ist unwahrscheinlich. Verantwortliche müssen der de[22] unverzüglich möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung gem. Art. 33 Abs. 3 DS-GVO die erforderlichen Informationen übermitteln. Die betroffene Person ist persönlich von der Verletzung zu benachrichtigen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (Art.34 Abs. 1 DS-GVO).

Ist eine der Bedingungen nach Art. 34 Abs. 3 DS-GVO erfüllt, ist eine Benachrichtigung der betroffenen Person nicht erforderlich.

2.8 Verzeichnis der Verarbeitungstätigkeiten

In Art. 30 DS-GVO ist vorgeschrieben, dass der Verantwortliche bzw. der Auftragsverarbeiter ein „Verzeichnis der Verarbeitungstätigkeiten“[23] führen müssen. Ähnlich dem bisherigen Verfahrensverzeichnis handelt es sich dabei um eine Dokumentation und Übersicht aller Verfahren, bei denen personenbezogene Daten verarbeitet werden. Die neue Verordnung sieht im Vergleich zur bisherigen Rechtslage zusätzliche Angaben vor, wie z. B. Name und Kontaktdaten des ggf. bestellten Datenschutzbeauftragten, Löschfristen und die TOM. Mustervordrucke und Ausfüllhinweise sind auf den einschlägigen Datenschutzportalen des Bundes und der Länder zu finden. Das Verzeichnis ist außerdem auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen. Allerdings fällt die noch im BDSG a. F. geregelte Pflicht weg, das Verzeichnis jedermann auf Anforderung zur Verfügung zu stellen.

2.9 Gemeinsame Datenverarbeitung

Nach Art. 26 DS-GVO ist es zukünftig auch zulässig, dass mehrere verantwortliche Stellen die erlaubte Datenverarbeitung gemeinsam durchführen können. Erforderlich ist hierzu eine transparente Vereinbarung, die die jeweiligen Zwecke und Verantwortlichkeiten sowie die Handhabung hinsichtlich der Betroffenenrechte festlegt. Betroffene können ihre Rechte aber weiterhin gegenüber jedem einzelnen Verantwortlichen geltend machen.

---

[21] Abrufbar unter: https://www.bundesversicherungsamt.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20180611Muster_83a.pdf

[22] Datenschutzbehörden und Rechts- bzw. Fachaufsicht der SV-Träger.

[23] Abrufbar unter: https://www.bvdnet.de/datenschutzkonferenz-veroeffentlicht-hinweise-und-muster-zum-verzeichnis-der-verarbeitungstätigkeiten-nach-artikel-30-ds-gvo

2.10 Auftragsverarbeitung

Gem. Art. 28 und 29 DS-GVO ist die Auftragsverarbeitung erlaubt. Darunter versteht man die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch einen Auftragsverarbeiter entsprechend den Weisungen des für die Verarbeitung Verantwortlichen auf Grundlage eines schriftlichen Vertrags. Darunter fallen z. B. Unternehmen, die ihre Daten bei einem externen Rechenzentrum speichern oder die eine externe Stelle mit der Erstellung etwa von Rechnungen beauftragen.

Die neuen Regelungen ähneln den Vorgaben des BDSG a. F., enthalten aber weitergehende Pflichten für beide Seiten[24]. Die Auftragsverarbeitung ist nur zulässig, wenn der Auftragsverarbeiter hinreichende Garantien für eine ordnungsgemäße Datenverarbeitung bietet. Art. 28 DS-GVO enthält eine umfangreiche Aufzählung von Regelungsinhalten sowie Rechte und Pflichten, die in dem Vertrag zwingend vereinbart werden müssen. Neu ist, dass auch der Auftragsverarbeiter ein „Verzeichnis der Verarbeitungstätigkeiten“ führen muss.

Datenverarbeitung und auch Auftragsverarbeitung ist in Drittstaaten – wie bisher – nur zulässig, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Die bisherige deutsche Restriktion, dass in Drittstaaten – auch bei angemessenem Datenschutzniveau – keine Daten der besonderen Art (z. B. Gesundheitsdaten) verarbeitet werden dürfen, entfällt nach der DS-GVO.

[24] Siehe FAQ des Bundesversicherungsamtes zur DS-GVO:
https://www.bundesversicherungsamt.de/fileadmin/redaktion/Datenschutz_Datensicherheit/20180522_DSGVO_FAQ_Version_5.pdf

3 Übertragung von Papierunterlagen in die elektronische Form

3.1 Allgemeines

Dieser Abschnitt des Leitfadens beschreibt das Scanverfahren, also die Überführung von Papierdokumenten in die elektronische Form. Die nachfolgenden Empfehlungen beziehen sich hauptsächlich auf folgende Themen:

- Klassifizierung von Papierdokumenten
- Dokumentation des Scan-Vorgangs
- Sicherungsmaßnahmen und
- Vernichtung der Originalbelege

Ziel dieses Abschnittes ist es, die gesetzlichen Vorgaben zu dieser Thematik zusammenzutragen und die hieraus abgeleiteten Anforderungen der Prüfdienste für die praktische Umsetzung zu formulieren. Die Anforderungen und Empfehlungen betreffen neu entwickelte und zukünftig realisierte Scanprojekte. Bereits etablierte Verfahren, die auf früheren Versionen des Leitfadens (und der darin zugrunde gelegten, teilweise außer Kraft gesetzten Vorschriften wie z. B. SigG und SigV) basieren, können nach Ansicht der Prüfdienste weiter betrieben werden.

Dieser Leitfaden ersetzt nicht die individuellen Risikoanalysen und das strukturierte Vorgehen bei der Auswahl, Einführung und (gesetzesmäßigen) Umsetzung konkreter Maßnahmen. Folgende Gesetze und Verordnungen sind für das Scanverfahren von besonderer Bedeutung:

- §§ 35 und 36a SGB I
- §§ 110a bis 110c SGB IV
- §§ 284 ff. SGB V
- §§ 67 ff. SGB X
- §§ 6 und 7 des Gesetzes zur Förderung der elektronischen Verwaltung (EGovG)
- Vertrauensdienstegesetz (VDG)
- Verordnung des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung)
- Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DS-GVO)
- Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (SVRV)
- Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung (SRVwV)

Des Weiteren sind folgende, vom Bundesamt für Sicherheit in der Informationstechnik (BSI), des Bundesbeauftragten für den Datenschutz und Informationsfreiheit (BfDI) und vom Bundesinnenministerium herausgegebenen Werke, Standards und Empfehlungen in den jeweils aktuellen Fassungen zu beachten:

- BSI-Standards 200-1, 200-2, 200-3 und 100-4
- IT-Grundschutzkompendium (Edition 2018)
- Technische Richtlinie TR-03138 „Ersetzendes Scannen“ (TR-RESISCAN)
- Technische Richtlinie TR-03125 „Beweiswerterhaltung kryptografisch signierter Dokumente“ (TR-ESOR)

Der Leitfaden verweist an den entsprechenden Stellen hierauf.

Empfohlen wird, für die Dateien der übertragenen Dokumente nur Dateiformate zu verwenden, die eine langfristige Lesbarkeit sicherstellen (TIFF bzw. PDF/A).

3.2 Übertragung in die elektronische Form

Das Übertragen von Papierdokumenten in die elektronische Form ist in § 110a SGB IV geregelt. Dieser Paragraph gilt als spezialrechtliche Norm vorrangig gegenüber der in § 7 EGovG enthaltenen Regelung. Ergänzend enthält das EGovG Hinweise darauf, wie das Scanverfahren technisch und organisatorisch auszugestalten ist, nämlich nach dem „Stand der Technik“. Dieser kann sich z. B. aus Richtlinien des BSI ableiten (siehe Minikommentar des BMI zu § 7 EGovG).

Die TR-RESISCAN beschreibt die technischen und organisatorischen Anforderungen für Scanprozesse und Scanprodukte, die erfüllt sein müssen, damit Papierdokumente rechtssicher und gerichtsverwertbar digitalisiert werden können.

Ziel der TR ist es, den Anwendern in Wirtschaft und Verwaltung einen Handlungsleitfaden und eine Entscheidungshilfe zum ersetzenden Scannen zu geben. Im Hinblick auf die Informationssicherheit werden die bei einem Scanprozess bedeutsamen Bedrohungen in einer Strukturanalyse für alle Datenobjekte und Kommunikationsbeziehungen systematisch dargestellt. Auf Grundlage einer darauf aufbauenden Schutzbedarfsanalyse und anhand der entlang der verschiedenen Scanphasen durchgeführten Risikoanalyse werden konkrete Sicherheitsmaßnahmen beschrieben.

Die TR enthält einen modularen Anforderungskatalog, der unterschiedliche Sicherheitsstufen umfasst. Während es in der „Basisstufe“ vor allem um einen grundsätzlich ordnungsgemäßen und mit grundlegenden Sicherheitsmaßnahmen ausgestalteten Scanprozess geht, werden in den „Ausbaustufen“ besondere Anforderungen an Integrität, Verfügbarkeit und Vertraulichkeit mit entsprechend erhöhten Sicherheitsmaßnahmen beschrieben.

Die nachfolgend aufgeführten Anforderungen an den Scanprozess leiten sich grundsätzlich aus dieser Richtlinie ab.

Die Prüfdienste des Bundes und der Länder werden die sich aus diesem Leitfaden sowie der TR-RESISCAN ergebenden Anforderungen bei Prüfungen als Prüf- und Bewertungsgrundlage heranziehen.

3.2.1 Scannen von Papierdokumenten

§ 110a SGB IV regelt, wie mit Papierdokumenten zu verfahren ist, die gescannt werden sollen. Diese sind durch ein maschinelles Scanverfahren in elektronische Dokumente zu übertragen. Hierbei sind folgende Besonderheiten zu beachten:

3.2.1.1 Klassifizierung der Papierdokumente

Der SV-Träger hat für die einzuscannenden Dokumente eine fachliche Schutzbedarfsanalyse zu erstellen, in der hinsichtlich der Schutzziele „Integrität“, „Vertraulichkeit“ und „Verfügbarkeit“ eine Klassifizierung vorzunehmen ist. Die TR-RESISCAN schlägt hier eine dreistufige Aufteilung in „normal“, „hoch“ und „sehr hoch“ vor.

Während für ein als „normal“ klassifiziertes Dokument einfache technisch-organisatorische Schutzmaßnahmen im Scanprozess implementiert werden müssen, fordert die TR für „hoch“ und „sehr hoch“ eingestufte Dokumente die Anwendung kryptographischer Sicherungsmittel.

Für den SV-Träger bedeutet dies, dass er unterschiedliche technisch-organisatorische Verfahren für jede Dokumentenklasse einführen müsste. Aufgrund des hohen Aufwandes erscheint eine solche Lösung nicht wirtschaftlich.

Die Prüfdienste empfehlen daher, das Scanverfahren so zu gestalten, als seien nur Dokumente mit Schutzbedarf „sehr hoch“ zu scannen. Nähere Ausführungen zu den Anforderungen an ein solches Scanverfahren sind der TR-RESISCAN und ihren Anhängen zu entnehmen.

3.2.1.2 Bildliche und inhaltliche Übereinstimmung

Die Wiedergabe auf einem Bildträger oder die Daten auf einem anderen dauerhaften Datenträger müssen mit der dieser zu Grunde gelegten schriftlichen Unterlage bildlich und inhaltlich vollständig übereinstimmen. Die Gesetzesbegründung führt dazu aus, dass die „Wiedergabe bei einem späteren Abruf einen vollständigen „urschrift-getreuen“ Ausdruck oder eine sonstige entsprechende Reproduktion garantiert“. Daraus könnte nunmehr abgeleitet werden, dass ausschließlich eine Farbabbildung mit qualifizierter elektronischer Signatur urkundliche Beweiskraft besitzt.

Die Prüfdienste des Bundes und der Länder sind der Auffassung, dass die SV-Träger aus Gründen der Rechtssicherheit alle papiergebundenen Dokumente in Farbe einscannen sollten. Lediglich bei Vordrucken, bei denen Farbe keine Beweiskraft besitzt sondern nur als Ausfüllhilfe für die spätere Texterkennung dient (z. B. AU-Bescheinigungen, Verordnungen), ist ein Farbscan entbehrlich.

Für die Prüfung von RSA-relevanten Belegen (z. B. Verordnungen) halten die Prüfdienste die Vorlage von Graustufen-Images mit allen Formatierungszeichen für ausreichend.

Die SV-Träger sollten sich an den Ergebnissen einer individuellen Risikobetrachtung orientieren, im Rahmen derer insbesondere die Gefahren des möglichen Verlustes der Beweiskraft von Graustufen-Wiedergaben mit den Folgen des größeren wirtschaftlichen Aufwandes bei der Digitalisierung in Farbe gegeneinander abzuwägen sind.

Obwohl es grundsätzlich keine eklatanten Preisunterschiede mehr zwischen Farb- und S/W-Scannern gibt - jeder Scanner beherrscht beide Verfahren - wäre jedoch erforderlich, dass der Scanner multistreamfähig ist. Das bedeutet, es werden beim Scanvorgang sowohl ein farbiges als auch ein S-/W-Image erzeugt. Während das farbige elektronisch signiert und archiviert wird, benötigt man das S-/W-Image nur für das Auslesen und die Nachbearbeitung der Daten. Dieses Image könnte nach dem Lesevorgang wieder automatisch gelöscht werden.

Zur Vermeidung einer erhöhten Netzwerkperformance wegen des Abrufs von Farbimages durch die Sachbearbeitung wäre auch eine weitere Nutzung des vorgenannten S-/W-Image möglich.

Es muss sichergestellt sein, dass die Belege urschriftgetreu gescannt werden. Dies erfordert auch, dass auf dem Original vorhandene Formatierungszeichen (z. B. Linien, Rahmen, Logos u.a.) auch auf dem signierten Image vorhanden sein müssen. Für das Auslesen der Rohdaten für die weitere maschinelle Verwendung (z. B. OCR-Lesung) kann auf diese Kriterien allerdings verzichtet werden.

Rückseiten sind beim Stapelsignaturverfahren grundsätzlich ebenfalls zu scannen. Ein automatisches Löschen leerer Rückseiten ist zulässig, sofern die Scansoftware gewährleistet, dass bereits bei einem auf der Rückseite befindlichen Zeichen (z. B. ein „Punkt“) ein automatisches Löschen ausgeschlossen ist.

Die Anbringung eines elektronischen Eingangsstempels bzw. einer automatischen Paginierung ist unmittelbar vor dem Scanvorgang zulässig. Nach dem Scanvorgang (auf dem Image) automatisch angebrachte elektronische Eingangsstempel sind nicht zulässig, da das Image dann kein originalgetreues Abbild des Urbeleges mehr ist. Dabei ist sicherzustellen, dass der elektronische Eingangsstempel dem tatsächlichen Eingangsdatum des Papierdokumentes entspricht. Es ist sicherzustellen, dass eingehende Schriftstücke, bei denen es sich offensichtlich um unbeglaubigte Kopien oder Papier-Faxe handelt, nicht automatisch gescannt und signiert werden. Vielmehr ist hier erforderlich, diese Schriftstücke vor dem Signiervorgang mit einem Stempelaufdruck „Kopie“ bzw. „FAX“ zu versehen.

Die Verwendung von Multi-TIFF-Dokumenten, bei denen ein aus mehreren Seiten bestehendes Dokument mit einer Elektronischen Signatur versehen wird, ist möglich. Vermieden werden sollte jedoch, mehrere unterschiedliche Dokumente mit einer einzigen Signatur zu versehen. Hierbei könnte das Problem auftreten, dass die einzelnen Dokumente unterschiedlich lange aufbewahrt werden müssen. Bei der Vernichtung eines dieser Dokumente müssten die anderen neu signiert werden.

Die Anforderungen gelten auch für über Apps erstellte Abbilder und deren Übermittlung sowie Speicherung beim SV-Träger.

3.2.1.3 Dokumentation des Scan-Vorgangs

Bis zum 31.12.2015 war in § 110d SGB IV geregelt, dass die beim Scan-Vorgang erzeugten Images vom Scan-Operator mit einer qualifizierten elektronischen Signatur (QES) signiert werden mussten. Nur dann konnte nachgewiesen werden, dass das Original vorlag und in die elektronische Form übertragen wurde.

Nach Wegfall der o.g. Vorschrift besteht gleichwohl die Notwendigkeit, festzustellen, wer das Dokument in die elektronische Form übertragen hat. Eine rechtliche Verpflichtung hierzu ergibt sich aus § 67b SGB X i.V.m. § 22 Abs. 2 Nr. 2 BDSG (siehe auch § 7 EGovG).

Der Integritätsschutz ergibt sich aus Art. 5 Abs.1 Buchst. f) DS-GVO: Daten müssen gegen unbeabsichtigte Schädigung durch geeignete technische und organisatorische Maßnahmen geschützt sein.

Wie bereits in Punkt 3.2.1.1 beschrieben, wird empfohlen, alle einzuscannenden Papierdokumente mit dem Schutzbedarf „sehr hoch“ zu klassifizieren und die daraus resultierenden Anforderungen gem. TR-RESISCAN umzusetzen. Hierzu gehört u.a.

- die Protokollierung, wer das Scansystem wann und in welcher Weise genutzt hat und
- der Einsatz kryptographischer Sicherungsmittel, z. B. der qualifizierten elektronischen Signatur (QES).

Um eine unerkannte nachträgliche Manipulation der während des Scanprozesses entstehenden Datenobjekte zu verhindern, müssen daher geeignete Mechanismen für den Schutz der Integrität dieser Datenobjekte eingesetzt werden (siehe auch Abschnitt 4, Punkt 4.3.2).

3.2.2 Formen der Signatur

<u>Einzelplatzsignatur:</u>
Mit Einführung der eIDAS-Verordnung wurde die Signaturrichtlinie aufgehoben; das Signaturgesetz wurde durch das Vertrauensdienstegesetz (VDG) abgelöst, das am 29.07.2017 in Kraft getreten ist. Auch die Signaturverordnung trat zum 29.07.2017 außer Kraft. Der Gesetzgeber ging

schon in der Vergangenheit (mit dem Signaturgesetz) davon aus, dass eine elektronische Signatur als Ersatz einer sonst erforderlichen körperlichen Unterschrift an einem einzelnen Dokument angebracht wird. Die entsprechenden Regelungen im SGB sehen daher vor, dass die Person, welche die Signatur auf einem Dokument anbringt, sich vor der Erzeugung der Signatur davon überzeugt, dass die Daten des zu signierenden Dokumentes integer sind. Klassischer Einsatzbereich ist der Sachbearbeiter-Arbeitsplatz (SB), an dem einzelne Dateien elektronisch signiert und versendet werden sollen.

Die Einzelplatzsignatur erfordert grundsätzlich, dass sich die hierzu benötigte Hardware (Kartenlesegerät) und Software (Signatursoftware) im direkten Zugriffsbereich des Anwenders befindet. Im Übrigen gelten hier dieselben Sicherheitsvorschriften, die auch bei sonstigen SB-Plätzen – gem. Dienstanweisung – zu beachten sind.

Stapelsignatur:
Beim Stapelsignaturverfahren werden große Mengen Beleggutes (z. B. AU-Meldungen) stapelweise eingescannt. Die erzeugten Images werden mit Hilfe einer Signaturanwendungskomponente an einen Scan-/Signaturarbeitsplatz übertragen, an dem der Signaturvorgang initiiert werden kann.

Der Vorteil dieses Verfahrens gegenüber dem der Einzelsignatur liegt im Zeitgewinn: Das Einscannen, Signieren und Speichern von Papierbelegen kann im Stapelbetrieb erfolgen. Dies erfordert, den Übernahmeprozess effizient zu gestalten. Hier entsteht ein Problem, wenn deshalb der vollständige Übernahmeprozess bestehend aus

- Scannen des Dokuments,
- Erstellen der Bilddatei und
- Signieren der Datei

automatisiert wird, so dass nicht davon ausgegangen werden kann, dass der Bediener jedes Dokument vor dem Signieren visuell auf Übereinstimmung prüft.

Die Prüfdienste empfehlen, unter Berücksichtigung von § 7 EGovG, dass der Signiervorgang grundsätzlich zeitlich und räumlich in unmittelbarem Zusammenhang mit dem Einscannen erfolgt. Die Signatur darf hierbei nur von der Person angebracht werden, die das Dokument auch in die elektronische Form überführt hat („Stapelsignatur“).

Alternativ dazu besteht die Möglichkeit, die Images unmittelbar nach deren Herstellung durch einen anderen als den Scan-Operator signieren zu lassen. Dieser hat aber vor dem Signiervorgang die Übereinstimmung der Unterlage mit Inhalt und Bild der Wiedergabe zu prüfen. Das bedeutet, jedes Image ist visuell zu prüfen. Eine Stapelsignatur ist bei dieser Alternative nur zulässig, wenn im Signiertool eine voll umfängliche (100 v. H.) Prüfung erfolgt.

Die Stapelsignatur wird erstmals in § 41 Abs. 5 SRVwV als „Massensignatur“ beschrieben und an verschiedene Voraussetzungen gebunden.

Da beim Stapelsignaturverfahren nicht mehr jeder einzelne eingescannte Beleg vor seiner Signatur einer visuellen Kontrolle unterzogen wird, muss durch bestimmte technische und organisatorische Vorkehrungen ein mögliches Schadensrisiko minimiert werden.

3.2.3 Sicherheitsmaßnahmen

Bei Verfahren zur Übertragung von Papierunterlagen in die elektronische Form (Scan- / Signaturverfahren) sind insbesondere folgende Sicherheitsmaßnahmen erforderlich:

Bauliche und technische Vorkehrungen:
Bei der Gestaltung der baulichen Maßnahmen ist zu unterscheiden zwischen

- Einzelplatzsignatur und
- Stapelsignatur.

Der Einsatz von Stapelsignaturverfahren hat ausschließlich in einer abgesicherten Umgebung zu erfolgen. Die auf der Homepage der BNetzA veröffentlichten Bestätigungen zum Einsatz von Signaturanwendungskomponenten verlangen, dass der Scan- / Signatur-Bereich sich in einem geschützten Einsatzbereich befindet. Dieser darf von außen nur mit Schlüssel / Karten von Berechtigten zu öffnen sein. In diesem Bereich sind unterzubringen:

- Scanner (für die Beleglesung)
- Scan- / Signatur-Arbeitsplätze

Einzelheiten sind der Homepage der BNetzA zu entnehmen.

Die Signaturanwendungskomponente ist derart zu konfigurieren, dass die Signaturerstellungseinheit lediglich für die Signatur eines Stapels freigeschaltet wird; die Stapelgröße sollte 250 (bei Hash-Bäumen = 256) Dokumente (es werden einzelne Dokumente und nicht Seiten signiert) nicht überschreiten.
Um mangelhafte Scanvorgänge (z. B. fehlende Seiten, mangelnde Lesbarkeit) zu erkennen, muss eine geeignete Qualitätskontrolle und bei Bedarf eine erneute Erfassung des gesamten Stapels stattfinden. Die detaillierte Ausgestaltung dieser Kontrolle soll sich am Schutzbedarf der verarbeiteten Dokumente, am Scan-Durchsatz sowie an der Zuverlässigkeit des Scansystems orientieren.

Bei der Verarbeitung von Dokumenten mit einem Schutzbedarf von „normal“ und bei hohem Durchsatz kann die Sichtkontrolle auf Stichproben reduziert werden, um systematische Fehler zu erkennen. Sie sollte aber mindestens das erste und das letzte Blatt des Stapels umfassen.

Hierzu muss die Signaturanwendungskomponente technische Vorkehrungen beinhalten, wonach der Scan-Operator gezwungen wird, einen festgelegten Stichprobenumfang einer visuellen Kontrolle zu unterziehen. Erst nach Durchführung der Sichtkontrolle der im System hinterlegten Mindeststichprobe kann der Stapel signiert werden.

Für die Signatur des nächsten Stapels muss der Scan-Operator seinen Signatur-PIN erneut eingeben. Eine Freischaltung der Signaturkarte für ein festgelegtes Zeitfenster ist nicht zulässig.

Um die Übersichtlichkeit für den Scan-Operator nicht zu erschweren, sollte technisch sichergestellt sein, dass maximal ein Rückstand von drei eingescannten, ungeprüften und unsignierten Stapeln vorhanden ist.

Um die Auslastung der Scan-Signatureinheiten zu erhöhen, kann ein Scan-Operator zeitgleich zwei Scan-Straßen bedienen. Hierbei ist sicher zu stellen, dass er je Scan-Straße über eine eigene Signaturerstellungskomponente verfügt.

Vor der endgültigen Langzeitspeicherung der signierten Images im Langzeitarchiv ist jede Signatur noch einmal (automatisch) auf Gültigkeit zu überprüfen. Dies kann durch eine Online-Abfrage beim Vertrauensdiensteanbieter oder gegen die auf dem Signaturserver gespeicherten (im Hause eingesetzten) Zertifikate sowie die aktualisierten Sperrlisten erfolgen.

Das Ergebnis der Überprüfung ist mit zu speichern. Sollten hierbei fehlerhafte Signaturen festgestellt werden, müssen alle nach dem Zeitpunkt der fehlerhaften Signatur eingescannten Dokumente erneut gescannt und signiert werden.

Es sei besonders darauf hingewiesen, dass der Einsatz einer automatischen Signatur voraussetzt, dass die technischen Komponenten so gewählt sind, dass der Ablauf nicht unterbrochen werden kann (Transaktionssicherheit).

Das Einscannen und Signieren geringer Papiermengen kann unter der Voraussetzung, dass eine Einzelsignatur an jedem Dokument angebracht wird, auch an den normalen Arbeitsplätzen erfolgen.

Darüber hinaus sind die allgemeinen – auch durch das BSI beschriebenen – Standards für die Herstellung der erforderlichen IT-Sicherheit für die Server und das Leitungsnetz zu beachten.

Organisatorische Vorkehrungen:
Der gesamte Verfahrensablauf vom Eingang der Papierbelege im Scan- / Signaturbereich bis zur Übertragung der Images in das elektronische Archiv sowie der Verbleib bzw. die Vernichtung der Papierbelege ist in einer Dienstanweisung (DA) detailliert zu beschreiben. Diese DA ist den Scan-Operatoren zur Kenntnis zu geben.

Eine Vernichtung der Papierdokumente kann nur dann vorgenommen werden, wenn die im SGB I und IV sowie der SVRV und SRVwV aufgeführten Voraussetzungen in allen Punkten erfüllt sind.

Es wird empfohlen, die Vernichtung erst nach der Nachbearbeitung, z. B. Plausibilitäts- und Mitgliedschaftsprüfung, durchzuführen und wenn sichergestellt ist, dass das Dokument im Archiv vorliegt / angekommen ist.

Es muss sichergestellt sein, dass unsignierte elektronische Dokumente bei fehlenden Originalunterlagen nicht nachträglich ausgedruckt und erneut dem System (jetzt mit Signatur) zugeführt werden können.

Beim nachträglichen Scannen von Altbeständen muss das Image den bereits im System gespeicherten Informationen zugeordnet werden.

Betriebssystem und Netzwerk:
Hinsichtlich der Konfiguration und des Betriebes von Scan- / Signaturlösungen haben die Prüfdienste des Bundes und der Länder in Zusammenarbeit mit dem BSI Rahmenbedingungen definiert, die insbesondere beim Einsatz der „Stapelsignatur“ zu beachten sind:

Grundsätzlich gelten hier die gleichen Sicherheitsstandards, die auch im täglichen „Normalgeschäft“ zu beachten sind.

Die im Stapelsignaturgeschäft erforderlichen Sicherheitsmaßnahmen erfordern, dass das Teilnetz, in dem die Scan- / Signatur-Operatoren tätig sind, vom übrigen Hausnetz zu trennen ist. Eine „Pseudotrennung“ durch Verwendung mehrerer Netzwerkkarten im Scanclient bietet aus Sicht des BSI keine hinreichende Sicherheit.

Es sind nur solche Verbindungen zulässig, die von innen nach außen aufgebaut werden können. Dies ist durch eine entsprechende Hardware-Firewall sicherzustellen. Eine Anbindung dieser Arbeitsplätze an das Internet sowie den zentralen Mail-Server ist unzulässig.

Die Verwendung einer Software-Firewall auf dem jeweiligen Rechner wird für nicht ausreichend angesehen, weil Schadsoftware dazu führen kann, dass die Maßnahme wirkungslos ist.

Maßgeblich für den Betrieb der Karten sind die durch die Bundesnetzagentur (BNetzA) festgelegten Anforderungen an die Einsatzumgebung.[25]

Dadurch ist es erforderlich, Kartenleser der Klasse 3 zu verwenden. Diese Geräte verfügen über ein Display, auf dem angezeigt wird, welche Daten vom User signiert werden.

Es sollte auf den WINS-Dienst verzichtet werden. Eine Auflösung der Rechnernamen auf IP-Adressen bzgl. Server und Mailserver sollte durch LMHOST-Eintrag sichergestellt werden.

Bei Windows-Terminal-Servern: Da das Signaturprogramm auf dem (entfernten) Server liegt, ist die PIN-Abfrage vom Terminal-PC mit einer Verschlüsselung bzw. durch den Einsatz von zugelassenen Verschlüsselungssystemen (www.bsi.bund.de) zu schützen. Maßgeblich ist, ob die Evaluierung und Bestätigung für die eingesetzte Karte den Einsatz über Terminalserver zulassen.

Zugriff auf die Systemzeit hat ausschließlich der Administrator. Wenn dies gewährleistet wird, kann auf den Einsatz eines (kostenpflichtigen) Zeitstempeldienstes verzichtet werden.

Auf dem Rechner dürfen keine E-Mail Programme (kein Internetanschluss) und keine Grafikbearbeitungsprogramme installiert sein.

Nicht wiederbeschreibbare Datenträger:
Die gesetzlichen Regelungen schreiben vor, dass eine elektronische Langzeitspeicherung auf Medien zu erfolgen hat, die nicht wieder beschreibbar sind.

§ 110a Abs. 2 SGB IV spricht von „dauerhaften Datenträgern“ und schränkt somit die Medienwahl nur hinsichtlich der Lebensdauer ein. Die Daten müssen während der Aufbewahrungsfristen verfügbar und jederzeit innerhalb einer angemessenen Frist wieder herstellbar sein. Somit spricht grundsätzlich auch nichts gegen die Verwendung von Tapes oder Harddisks.

Voraussetzung für die Langzeitspeicherung auf diesen Medien ist jedoch die Gewährleistung einer Versionsintegrität (WORM-Prinzip). Ein auf Harddisks langzeitarchiviertes, qualifiziert signiertes Image darf bei Aufruf durch den User nicht verändert werden (können); in diesem Fall ist automatisch eine Kopie des Images zu erzeugen, die dann unter einer neuen Versionsnummer abgespeichert wird. Hierdurch wird die Revisionssicherheit der signierten Dokumente gewährleistet. Die Möglichkeit des physikalischen Löschens nach Ablauf der gesetzlich vorgeschriebenen Aufbewahrungsfrist muss vom SV-Träger in der Dienstanweisung detailliert festgelegt werden (u. a. Zeitpunkte und Zuständigkeiten).

Fernwartung:
Aufgrund der besonderen Sicherheitsanforderungen für die technische Anbindung der im Scan-Signaturbereich eingesetzten Hard- und Software erscheint eine Fernwartung der Geräte als problematisch.

Für eine Fernwartung sind die durch das BSI in den „IT-Grundschutz-Katalogen“ festgelegten Standards wie Call-Back-Verfahren und der Einsatz von Einmal-Passworten zu beachten. Grundlage für die zu wählenden Maßnahmen ist der jeweilige Schutzbedarf (normal, hoch, sehr hoch) der zu scannenden Dokumente.

---

[25] BNetzA „Einheitliche Spezifizierung der Einsatzbedingungen für Signaturanwendungskomponenten“; abrufbar unter: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/SpezifiziergEinsatzBedinggn15pdf.pdf?__blob=publicationFile&v=1

Darüber hinaus ist organisatorisch sicherzustellen, dass eine Fernwartung ausschließlich in Zeiten erfolgt, in denen kein Scan-Signatur-Betrieb stattfindet.

3.2.4 Vernichtung von Originalbelegen

Für die Vernichtung von Originaldokumenten / Akten gelten folgende Rechtsgrundlagen:

- § 110b SGB IV
- § 80 SGB X
- Art. 32 DS-GVO

Die Vernichtung der Originalpapierbelege ist in einer Dienstanweisung zu regeln. Frühester möglicher Zeitpunkt für die Vernichtung ist die vollständige elektronische Aufbewahrung und Sicherung der Images und zugehörigen Signaturen. Die Ordnungsmäßigkeit ist von der internen Revision in regelmäßigen Abständen zu prüfen.

In Fällen der „frühen Signatur“ (z. B. beim Posteingang) wird empfohlen, die papiergebundenen Dokumentationen solange aufzubewahren bis die Sachbearbeitung die Zuständigkeit geklärt hat.

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben eine datenschutzgerechte Verarbeitung der Daten sicherzustellen. Die letzte Phase der Datenverarbeitung ist das Löschen gespeicherter Daten bzw. das Vernichten von Datenträgern. Datenträger können z. B. Festplatten, Magnetbänder, Filmmaterial, Disketten, CDs, DVDs, USB-Sticks, Chipkarten oder Papier sein.

Die datenschutzgerechte Vernichtung ist in der DIN 66399 „Büro- und Datentechnik - Vernichtung von Datenträgern“ geregelt. Die dreiteilige Norm hat die seit 1995 geltende DIN 32757-1 abgelöst und wird damit auch digitalen Dokumenten bzw. Datenträgern und den damit verbundenen Sicherheitserfordernissen gerecht. Ebenfalls gilt die Europäische Norm EN 15713 „Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln“. Sie enthält im Vergleich zur älteren DIN 32757-1 zwar Vorgaben für weitere Datenträger neben dem Papier, aufgrund ihrer teilweise wenig verbindlichen Formulierungen kann sie nur eingeschränkt als Maßstab herangezogen werden.

Die Teile eins und zwei der DIN 66399 (gültig ab Oktober 2012) enthalten die Grundlagen und Begriffe sowie die Anforderungen an Maschinen; Teil drei DIN SPEC 66399-3 (gültig ab Februar 2013) gibt die Spezifizierung der während der Vernichtung zu beachtenden Prozessschritte vor, um so die Absicherung des Gesamtprozesses der Datenträgervernichtung zu gewährleisten.

Neu sind die drei Schutzklassen, die jetzt zusammen mit den Sicherheitsstufen der Klassifizierung der anfallenden Daten dienen. Bei der Ermittlung des Schutzbedarfs für die Vernichtung der Datenträger ist der Grad der Schutzbedürftigkeit dabei ausschlaggebend für die Sicherheitsstufe. Es werden insgesamt sechs unterschiedliche Materialklassifizierungen verwendet. Sie berücksichtigen auch die Größe der Informationsdarstellung auf den Datenträgern. Weiterhin werden in der DIN 66399 statt bisher fünf Sicherheitsstufen jetzt sieben definiert.

Sozialdaten sind nach derzeitiger Auffassung der Prüfdienste nach Schutzklasse 3 (sehr hoher Schutzbedarf) zu vernichten. Zusätzlich können in den jeweiligen Einsatzgebieten landes- bzw. bereichsspezifische Spezialvorschriften gelten. Die Einstufung muss sich aus wirtschaftlichen / organisatorischen Gründen immer nach dem zu vernichtenden Gut richten, welches der höchsten Schutzklasse angehört.

Zur Vernichtung von Datenträgern kann eine andere Stelle beauftragt werden. Dabei handelt es sich um einen anzeigepflichtigen Auftrag gem. § 80 SGB X. Hierbei ist zu gewährleisten, dass Sozialdaten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen der Auftraggeber verarbeitet werden können (Auftragskontrolle). Der Auftrag zur Löschung personenbezogener Daten, die Weisungen zu technischen und organisatorischen Maßnahmen sowie die Zulassung von Unterauftragsverhältnissen sind daher schriftlich festzuhalten.

3.3 Einzelne Umsetzungsfragen

3.3.1 Umgang mit papierhaften Faxsendungen

Fax-Sendungen, die bei dem SV-Träger auf einem „Stand-Alone-Faxgerät“ eingehen und ausgedruckt werden, müssen – sofern der Absender keine Header-Informationen mitgesandt hat – mit einem Eingangs- und Faxstempel gekennzeichnet werden. Derartige Dokumente werden von den Prüfdiensten uneingeschränkt anerkannt, sofern

- das ausgedruckte Fax archiviert wird oder
- die Ausdrucke unmittelbar nach dem Ausdruck eingescannt und das Image mit einer QES versehen im elektronischen Langzeitarchiv gespeichert werden.

Werden eingehende Papier-Faxe ausgedruckt und an eine andere Dienststelle per Fax weitergesandt, so können diese „Fax-Kopien“ bei einer Prüfung nicht anerkannt werden. Bei diesen Dokumenten ist nicht feststellbar, ob zwischen Ausdruck und „weiterfaxen“ eine bildhafte Änderung am Original-Fax vorgenommen worden ist.

3.3.2 Verfahrensbeschreibung

Zur Beurteilung der vom SV-Träger vorgesehenen Verfahren ist die Vorlage von ausführlichen und nachvollziehbaren Verfahrensbeschreibungen unumgänglich. Solche müssen insbesondere detaillierte Informationen zu den Arbeitsabläufen (Geschäftsprozesse), den betroffenen Dokumentarten und Formularen, zu Datenschutz- und Datensicherheitsmechanismen, zur Karten- und Rechteverwaltung sowie zur Aufbewahrung, Löschung und Vernichtung beinhalten.

Der Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte und die Innenrevision sollten bei der Erstellung beteiligt werden.

3.3.3 Dienstanweisung

Nach § 17 SVRV i.V. mit § 40 SRVwV – die Anpassung auf die DS-GVO hat noch nicht für alle Gesetze stattgefunden – erlässt der Versicherungsträger bei Einsatz der automatisierten Datenverarbeitung zur Sicherheit des Verfahrens eine Dienstanweisung.

In der Dienstanweisung sind Regelungen u. a. zu folgenden Punkten zu treffen:

<u>Zertifikate:</u>

- Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert

der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen (§ 15 VDG).

Kartenmanagement:[26]
- Kartenausgabe / -ersatz (bei Verlust, Zerstörung, Vergessen)
  Anmerkung: Gem. § 14 VDG kann der SV-Träger selbst – neben dem Karteninhaber – eine Sperre der Karte bzw. des Zertifikats veranlassen. Ggf. sind entsprechende vertragliche Regelungen gem. § 12 Abs. 1 VDG mit dem Vertrauensdiensteanbieter zu treffen.
- Ggf. Ersatzkarten für alle Beschäftigten
- Stellvertretungsregelungen

Beschreibung des Scan- und Signaturverfahrens:
- Besonderheiten, z. B. Vorkehrungen / Regelungen zur Vermeidung von Doppelerfassungen

Zugriffs- und Zutrittsregelungen:
- Steuerung über Attributbeschreibungen/-inhalte
- Protokollierung und regelmäßige Auswertung der Zugriffe
- Zutritt zu den zentralen Scan- / Signaturarbeitsplätzen bei Einsatz der Stapelsignatur (Closed-Shop-Betrieb)

Regelmäßige Stichprobenprüfung von Signaturen:
- Täglich
- Umfang der Stichprobe, Auswahl der Stichprobe

Verpflichtungserklärung der Beschäftigten:
- Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen
- Der Signaturschlüssel-Inhaber muss gegenüber dem SV-Träger zustimmen, dass sein Zertifikat beim Zertifizierungsdiensteanbieter abrufbar gehalten wird (§ 12 Abs. 1 VDG)
- Verhalten in besonderen Situationen, z. B. wenn die Smartcard trotz Verbot mit nach Hause genommen und dort vergessen wird
- Prüfung arbeits- / dienstrechtlicher Konsequenzen, wenn Beschäftigte die Smartcard trotz Verbot mit nach Hause genommen und dort vergessen haben

Ergonomie der Arbeitsplätze:
- Scan- / Signaturarbeitsplatz mit einem Bildschirm, auf dem das gesamte Dokument komplett abgebildet werden kann
- Schulung der Benutzer und IT-Betreuer

3.3.4 Regelungen für das Kartenmanagement

Im Rahmen des elektronischen Geschäftsverkehrs werden Signaturkarten nur an den speziellen Arbeitsplätzen benötigt, an denen die Signatur eingescannter Belege oder elektronisch erstellter Dokumente erfolgt. Diese Arbeitsplätze sind nur funktionsfähig, wenn der Bediener auf seine gültige(n) Signaturkarte(n) zurückgreifen kann. Gem. § 41 Abs. 2 SRVwV sind Attributzertifikate zwingend vorgeschrieben; durch diese wird die Verwendung der Karte auf den jeweiligen Einsatzbereich beschränkt.

[26] Siehe Ausführungen zu Punkt 3.3.4.

Die Signaturkarten sollten in einem Bestandsverzeichnis verwaltet werden, so dass immer nachvollziehbar ist, wann welche Karten eingesetzt wurden. Außerdem können dann die Karten der Nutzer, die nicht mehr in dem jeweiligen Bereich tätig sind, gesperrt werden. Auf die besonderen Regelungen zur elektronischen Zahlungsanordnung (§ 11 Abs. 4 SRVwV) wird hingewiesen.

Auf Grund der Abhängigkeit von den Signaturkarten könnte für jeden Nutzer eine Reservekarte vorgehalten werden (gilt insbesondere bei „Stapelsignaturbetrieb"), sofern nicht durch andere organisatorische Regelungen die Aufrechterhaltung des Scan- / Signaturbetriebes gewährleistet ist. Die Notwendigkeit sollte der SV-Träger im Rahmen einer Risikobetrachtung feststellen. Die Verwendung einer allgemein nutzbaren Reservekarte ist nicht möglich, da die Signaturkarten personenbezogen ausgestellt werden. Mit dem Trustcenter sollten vertragliche Regelungen getroffen werden, dass Ersatzkarten in vertretbarer Zeit geliefert werden können.

Signaturkarten sollten an einem festen Platz aufbewahrt werden, z. B. in einem Schließfachsystem, aus dem die Nutzer sie bei Dienstbeginn entnehmen und bei Dienstende zurücklegen. Die Karten verlassen somit nie den gesicherten Bereich.

3.3.5 Langfristige Beweiserhaltung nach § 15 VDG

Neusignierung von Elektronischen Signaturen:
Elektronische Signaturen basieren auf mathematischen Komplexitätsproblemen. Der technische Fortschritt führt dazu, dass immer komplexere solcher Probleme im Laufe der Zeit gelöst werden können und somit ein Signaturalgorithmus insgesamt oder eine gegenwärtig als sicher angesehene Parametrisierung (hierzu zählt z. B. die Länge eines Schlüssels) ab einem bestimmten Zeitpunkt nicht mehr als sicher angesehen werden kann. Die elektronische Signatur verliert also durch den technischen Fortschritt im Laufe der Zeit ihre Sicherheits- und Beweiseignung, wenn nicht weitergehende Maßnahmen ergriffen werden. Insbesondere bei der Langzeitspeicherung wird sich dieser Fall häufiger ergeben.

Mit § 15 VDG hat der Gesetzgeber hierfür eine entsprechende Regelung geschaffen: „Sofern hierfür Bedarf besteht, sind qualifiziert elektronisch signierte, gesiegelte oder zeitgestempelte Daten durch geeignete Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die neue Sicherung muss nach dem Stand der Technik erfolgen."

Mit der Aufhebung des Signaturgesetzes und der Signaturverordnung entfiel die bisherige gesetzliche Grundlage für den Algorithmenkatalog, der letztmals am 30.12.2016 im Bundesanzeiger veröffentlicht wurde (BNetzA, 2016). Eine Weiterentwicklung des Algorithmenkatalogs in Form eines unverbindlichen Dokuments, das die Vorgaben des Algorithmenkatalogs in Form unverbindlicher Empfehlungen zum Stand der Technik fortschreiben würde, wurde als nicht sinnvoll angesehen. Stattdessen wurde primär auf die Empfehlungen des SOG-IS-Kryptokataloges[27] (SOG-IS, 2016) verwiesen.

[27] Quelle BNetzA:

https://www.bundesnetzagentur.de/DE/Service-Funktionen/ElektronischeVertrauensdienste/HinweiseEmpfehlungen/Empfehlungen/Empfehlungen_node.html

https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/Empfehlungen2018.pdf

Die erneute Signatur mit neuen Algorithmen und zugehörigen Parametern muss zu einem Zeitpunkt erfolgen, in dem die alte Signatur noch sicher ist. Um zu beweisen, dass dieses sog. Übersignieren rechtzeitig erfolgt ist, muss ein qualifizierter Zeitstempel angebracht werden. Wird dieses Verfahren regelmäßig angewendet, kann der Beweiswert und die Beweiseignung einer elektronischen Signatur noch nachgewiesen werden, auch wenn die Ursprungssignatur alleine zwischenzeitlich unsicher geworden ist. Die neu anzubringende Signatur muss dabei natürlich nicht von der Person angebracht werden, die die Ursprungssignatur erzeugt hat.

Neusignierung von Hashalgorithmen:
Genauso wie bei der erstmaligen Signatur geht es bei der Neusignatur auch darum, sie effektiv und kostengünstig durchzuführen. Das Übersignieren soll handhabbar sein und die Anzahl der notwendigen Zeitstempel gering gehalten werden.

Auch bei der Übersignatur wird nicht das Dokument selbst, sondern der Hashwert signiert. Problematisch hinsichtlich des Erhalts der dauerhaften Beweiseignung ist, dass auch die Hashalgorithmen mathematische Komplexitätsprobleme darstellen, die durch den technischen Fortschritt hinsichtlich der Sicherheit genauso beeinflusst werden, wie die elektronischen Signaturalgorithmen.

Wird ein Hashalgorithmus ab einem bestimmten Zeitpunkt nicht mehr als sicher eingestuft, so gelten auch hier die Bestimmungen aus §15 VDG; d. h., es ist ein erneuter Hashwert mit einem als sicher beurteilten Verfahren (für jedes Dokument) zu bilden, mit einer qualifizierten Signatur (neue Signaturalgorithmen und Parameter) zu signieren und ein qualifizierter Zeitstempel anzubringen.

Neusignierung von Zeitstempeln:
Sollte der qualifizierte Zeitstempel, sofern er selber auf einer qualifizierten Signatur beruht, unsicher werden, reicht es aus, den Hashwert über die archivierten Dokumente zu erzeugen, alle früheren Signaturen dabei mit einzuschließen und dann einen solchen sog. kryptografischen Zeitstempel (qualifizierte Zeitstempel der auf einer qualifizierten Signatur beruht) für diesen Hashwert einzuholen.

Vorausgesetzt, die Signatur, die der Zeitstempel trägt, basiert auf den neuen Algorithmen und Parametern, entfällt in diesem Fall die Notwendigkeit, nochmals eine eigene qualifizierte Signatur anzubringen.

Um eine Beweiswirkung zu erhalten, haben die SV-Träger rechtzeitig eine Nachsignatur zu veranlassen.

Nehmen SV-Träger die Nachsignatur bis zu dem im SOG-IS-Katalog genannten Termin nicht vor, fällt der Vorteil des Anscheinsbeweises (Privileg des Beweises des ersten Anscheins) weg. Für den SV-Träger tritt im Streitfall die Umkehr der Beweislast ein.

Der SOG-IS-Katalog unterscheidet zwischen empfohlenen Verfahren und Legacy-Mechanismen. Die Nutzung der Legacy-Mechanismen wird nicht empfohlen, da sie nicht mehr in vollem Umfang dem kryptographischen Stand der Technik entsprechen. Ihr Einsatz genügt aber bis zu dem Zeitpunkt des Auslaufens ihrer Eignung den Anforderungen[28].

Aus der Literatur können verschiedene Empfehlungen zur Vorgehensweise entnommen werden, die auch zur Wirtschaftlichkeit der Maßnahmen beitragen. U.a. ist als eine technische Mög-

[28] Siehe hierzu Abschnitt 1.1 von (SOG-IS, 2016).

lichkeit der Aufbau von Hashbäumen in Betracht zu ziehen (vgl. u.a. ArchiSig-Konzept).[29] Dazu muss das Dokument mit der Signatur, dem Zeitstempel sowie ggf. vorhandener Auskünfte aus dem Verzeichnisdienst exportiert werden. Daraus können die jeweiligen Archivcontainer gebildet werden (in diesem Fall ist im Container nur ein Dokument enthalten), über die dann die Hashbäume aufgebaut werden.

Als Alternative käme auch eine „große“ Containerlösung (hier sind mehrere Dokumente zusammengefasst) in Betracht, wenn eine an den Aufbewahrungsfristen orientierte Archivstruktur möglich ist.

Besonders für die langen Zeitspannen, wie sie für die Langzeitspeicherung notwendig sind, können keine verlässlichen Voraussagen der technischen Entwicklung getroffen werden.

Das Archiv sollte daher zumindest die verschiedenen Verfahren zur Neusignierung beherrschen.

[29] Roßnagel / Schmücker (Hrsg.) Beweiskräftige elektronische Archivierung, Economica Verlag, Heidelberg 2006, S. 86 ff.

4 Elektronische Kommunikation zwischen SV-Trägern und Versicherten

4.1 Grundsätze

Das zum 01.08.2013 in Kraft getretene „Gesetz zur Förderung der elektronischen Verwaltung sowie zur Änderung weiterer Vorschriften“ (EGovG) sieht vor, dass durch den Abbau bundesrechtlicher Hindernisse die elektronische Kommunikation mit der Verwaltung erleichtert wird. Medienbruchfreie Prozesse vom Antrag bis zur Langzeitspeicherung sollen möglich werden.

Das EGovG präzisiert die wesentlichen Verfahrensschritte, die eine vereinfachte, aber rechtssichere, Informationsbeschaffung, Kommunikation und Antragstellung über das Internet zulassen.

Nachfolgend werden die Abschnitte aus dem EGovG dargestellt, die eine erhebliche Relevanz im Hinblick auf die Online-Kommunikation zwischen SV-Trägern und ihren Versicherten / Arbeitgebern haben. Zur Orientierung bei der Auslegung der Rechtsvorschriften können auch die Ausführungen des BMI in seinem „Minikommentar“ zum EGovG herangezogen werden.

Neben der Kommunikation über Online-Medien, gewinnt die Kommunikation über Softwareprogramme, die speziell für die Nutzung auf mobilen Endgeräten geeignet sind (sog. Apps)[30], an Bedeutung. Allgemein gelten die Aussagen / Grundsätze zur elektronischen Kommunikation über Online-Medien auch für die Apps. Dies gilt insbesondere für folgende Anforderungen, die auch beim Angebot von Apps durch die SV-Träger erfüllt sein müssen:

- Sicherer Zugang (Authentifizierung)
- Nichtveränderbarkeit / Integrität übermittelter Daten
- Einhaltung allgemeiner und spezifischer Vorgaben zu Datenschutz und Datensicherheit
- Sichere Datenwege
- Revisionssichere Speicherung / Archivierung von übermittelten Daten

In diesem Kapitel werden daher Ausführungen zu Apps aufgenommen und Hinweise gegeben, sofern hierzu besondere / spezielle Anforderungen bestehen.

4.1.1 Geltungsbereich

Gem. § 1 Abs. 1 gilt das EGovG für die öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Bundes einschließlich bundesunmittelbarer Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Soweit das Gesetz den Anwendungsbereich einzelner Regelungen nicht explizit auf Behörden des Bundes beschränkt, gelten sie für alle Behörden, wenn sie Bundesrecht ausführen (§ 1 Abs. 2 EGovG).

Der Begriff der Behörde lehnt sich an die weite Definition des § 1 Abs. 2 SGB X an. Der Begriff der öffentlich-rechtlichen Verwaltungstätigkeit wird hier ebenso verwendet wie im SGB X.

Das EGovG gilt nicht, soweit Rechtsvorschriften des Bundes inhaltsgleiche oder entgegenstehende Bestimmungen enthalten (§ 1 Abs. 4 EGovG). Hierunter fallen z. B. die Regelungen zur rechtssicheren Übertragung von Papierdokumenten in die elektronische Form sowie die Langzeitspeicherung elektronisch erzeugter Dokumente. Diese sind in ihrem jeweiligen Anwen-

[30] Solmecke/Taeger/Feldmann (Hrsg.) Mobile Apps, Kap. 1 Rn. 14, S. 3.

dungsbereich vorrangig gegenüber den in § 7 EGovG getroffenen Regelungen zum Übertragen und Vernichten des Papieroriginals.

Nur für Behörden des Bundes / bundesunmittelbare Körperschaften geltende Regelungen:	Für Behörden des Bundes / Landes und für bundes- / landesunmittelbare Körperschaften geltende Regelungen:
§ 2 Abs. 2: Eröffnung De-Mail-Zugang	§ 2 Abs. 1: Eröffnung eines Zugangs zur elektronischen Kommunikation
	§ 3: Information über Behörden und ihre Verfahren
	§ 4: Elektronische Bezahlmöglichkeiten
	§ 5: Nachweise
§ 6: Elektronische Aktenführung	
§ 7: Übertragung und Vernichtung des Papieroriginals	
§ 8: Akteneinsicht	
§ 9: Optimierung von Verwaltungsabläufen und Information zum Verfahrensstand	
§ 11: Gemeinsame Verfahren	
	§ 12: Anforderungen an das Bereitstellen von Daten
	§ 13: Elektronische Formulare
	§ 14: Georeferenzierung
	§ 15: Amtl. Mitteilungs- u. Verkündungsblätter
§ 16: Barrierefreiheit	

Darüber hinaus sind insbesondere Regelungen des SGB I, SGB IV, SGB V und des SGB X sowie der DS-GVO zum Sozialdatenschutz vorrangig.

Weitere Vorschriften des Sozialversicherungsrechtes, die Berührungspunkte zum EGovG enthalten, sind u.a. § 35 SGB I i. V. m. § 80 SGB X, Art. 28 DS-GVO, § 36a SGB I, §§ 21, 25 SGB X.

Sofern landesunmittelbare SV-Träger diese Verfahren einführen wollen, sollten die im EGovG aufgeführten Grundlagen und Bedingungen beachtet werden. Weiterhin sollten die landesunmittelbaren SV-Träger laufend beobachten, ob einzelne Bundesländer entsprechende Vorschriften einführen.

4.1.2 Schriftformerfordernis und Ersatz der Schriftform

Nach § 126a BGB muss eine Urkunde vom Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden, wenn durch Gesetz die schriftliche Form vorgeschrieben ist. Der Umkehrschluss, dass immer dann, wenn eine Unterschrift vorgeschrieben ist, damit die gesetzliche Schriftform angeordnet ist, kann weder aus dem Wortlaut noch aus dem Zweck der Norm hergeleitet werden. Unterschriften werden im täglichen Leben auch außerhalb gesetzlicher Schriftformerfordernisse zu verschiedensten Zwecken geleistet und sind insbesondere als Feld für die Unterschrift des Erklärenden üblicher Bestandteil jeglicher Art von Formularen.

In den §§ 36a Abs. 2a SGB I, 13 EGovG wird klargestellt, dass kein Schriftformerfordernis vorliegt, wenn dieses nicht explizit in der Norm angeordnet wird:

> *„Ist durch Rechtsvorschrift die Verwendung eines bestimmten Formulars vorgeschrieben, das ein Unterschriftsfeld vorsieht, wird allein dadurch nicht die Anordnung der Schriftform bewirkt. Bei einer für die elektronische Versendung an die Behörde bestimmten Fassung des Formulars entfällt das Unterschriftsfeld.“*

Ist eine solche Schriftform jedoch explizit angeordnet, kann in der „elektronischen Welt“ auch

künftig eine Unterzeichnung **ausschließlich** über die QES oder eine der mit dem EGovG eingeführten schriftformersetzenden Technologien abgebildet werden.

Die Schriftform kann nach § 36a Abs. 2 Sätze 4 und 5 SGB I ersetzt werden durch:

- Die Bereitstellung **elektronischer Formulare über Web-Portale** der Behörde, die die Versicherten online „ausfüllen" können. Die Authentifizierung des Absenders muss hierbei über die eID-Funktion des neuen Personalausweises (nPA) oder den elektronischen Aufenthaltstitel (eAT) erfolgen (Nr. 1).
- Die **Übersendung von elektronischen Dokumenten per De-Mail** mit der Versandoption „absenderbestätigt", welche eine „sichere Anmeldung" voraussetzt. Dabei ist der Sender der Nachricht durch ein sicheres Authentifizierungsverfahren identifiziert und die Nachricht einschließlich aller Metadaten durch eine vom De-Mail-Diensteanbieter aufgebrachte QES (des De-Mail-Diensteanbieters) gegen Veränderungen geschützt (Nr. 2 und 3).
- Daneben können per Rechtsverordnung weitere ausreichend sichere Verfahren als Schriftformersatz festgelegt werden (Nr. 4).
- In der Kommunikation zwischen den Versicherten und ihren Krankenkassen kann die Identität auch mit der **elektronischen Gesundheitskarte** nachgewiesen werden (Satz 5).

Für alle anderen Formulare, für die **kein Schriftformerfordernis** besteht und die der Behörde elektronisch übermittelt werden sollen, ist dies **ohne Unterschrift** möglich (z. B. am Bildschirm ausgefüllte PDF-Dokumente). Für diese Dokumente / Daten können jedoch erhöhte Anforderungen bzgl. des Nachweises der Authentizität des Absenders und die Integrität bei der Datenübermittlung gegeben sein. Nähere Ausführungen sind dem Punkt 4.2.3 zu entnehmen.

Das Ausdrucken eines online ausgefüllten Formulars, das Unterschreiben sowie das Übersenden per Post sind bei Einhaltung dieser Anforderungen nicht mehr erforderlich.

Hinweis:
Sind in **Papierform ausgegebene Formulare** mit einem Unterschriftfeld versehen, sind diese Formulare von den Versicherten weiterhin zu unterschreiben.

4.1.3 Lesbarkeit übermittelter Dokumente

Ist ein der Behörde übermitteltes elektronisches Dokument für sie zur Bearbeitung nicht geeignet, teilt sie dies dem Absender unter Angabe der für sie geltenden technischen Rahmenbedingungen unverzüglich mit. Macht ein Empfänger geltend, er könne das von der Behörde übermittelte elektronische Dokument nicht bearbeiten, übermittelt sie es ihm erneut in einem geeigneten elektronischen Format oder als Schriftstück (§ 36a Abs. 3 SGB I).

4.1.4 Barrierefreiheit

Nach § 16 EGovG sollen die Behörden des Bundes die barrierefreie Ausgestaltung der elektronischen Kommunikation und der Verwendung elektronischer Dokumente nach § 4 des Behindertengleichstellungsgesetzes (BGG) in angemessener Form gewährleisten.

In dieser Vorschrift hat der Bundesgesetzgeber Regeln zur Herstellung von Barrierefreiheit in der Informationstechnik für die Verwaltung gesetzt. Damit ist die Verwaltung verpflichtet, ihre öffentlich zugänglichen Internetangebote grundsätzlich barrierefrei zu gestalten. Die entsprechende Rechtsverordnung „Barrierefreie Informationstechnikverordnung" (BITV) vom Bundesinnenministerium und Bundesministerium für Arbeit und Sozialordnung regelt die Vorgaben hierzu. Die Länder haben entsprechende Regelungen erlassen.

Danach sollen einzelne Komponenten der elektronischen Verwaltung, z. B. der elektronische Zugang zur Verwaltung und die elektronische Aktenführung, so gestaltet werden, dass die elektronischen Kommunikationseinrichtungen und elektronischen Dokumente für Menschen mit Behinderungen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar sind. Das ist dann der Fall, wenn ihnen der Zugang mit den hierfür vorhandenen, der jeweiligen Behinderung entsprechenden Hilfsmitteln möglich ist.

Hieraus ergeben sich folgende Grundsätze:

- Inhalte und Erscheinungsbild sind so zu gestalten, dass sie für alle wahrnehmbar sind.
- Die Benutzeroberflächen der Angebote sind so zu gestalten, dass sie für alle bedienbar sind.
- Inhalte und Bedienung sind so zu gestalten, dass sie allgemeinverständlich sind.
- Die Umsetzung der Inhalte soll so erfolgen, dass sie mit heutigen und zukünftigen Technologien funktionieren.

4.1.5 Datenschutzrechtliche Einschränkungen - Grundsatz

Die mit dem EGovG eingeführten Erleichterungen bei der Übermittlung elektronischer Dokumente oder Daten erreichen dort ihre Grenze, wo es sich um besonders schützenswerte Inhalte handelt. Hierunter fallen insbesondere sensible medizinische Angaben und Dokumente (Art. 9 Abs. 1 DS-GVO).

Sowohl bei der Beantwortung von Gesundheitsfragen in der Bildschirmmaske einer Web-Anwendung als auch beim Hochladen ärztlicher Dokumente können bestimmte technische Zusatzmaßnahmen der Datensicherheit und des Zugangs gefordert sein, die über die im EGovG genannten Bedingungen der datenschutzrechtlich „einfachen“ Kommunikation hinausgehen.

In den Artikeln 5, 12, 25, 32 und 35 DS-GVO finden sich grundlegende Anforderungen an die Sicherheit der Verarbeitung personenbezogener Daten. Die Verordnung fordert geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1). Mit dem Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17. Juli 2017 sind die Anforderungen aus der DS-GVO in das SGB X eingeflossen.

Je schützenswerter die Daten sind, desto strenger sind die technisch-organisatorischen Maßnahmen, die die verantwortliche Stelle einhalten muss. Bei bestimmten personenbezogenen Daten wie zum Beispiel Gesundheitsdaten, spielt besonders die Vertraulichkeit eine große Rolle. Unbefugte dürfen in keinem Fall Kenntnis von diesen Daten erhalten. Bei der elektronischen Kommunikation wird die Vertraulichkeit dadurch gewährleistet, dass die Nachricht und ihre Anhänge mit einer geeigneten Software verschlüsselt und besondere Anforderungen an die Authentifizierung erfüllt werden. Betroffen sind hiervon alle besonders schutzbedürftigen personenbezogenen Daten, also solche, die potentiell eine besondere Sensibilität aufweisen.

Art. 35 DS-GVO erfordert bei der Verwendung neuer Technologien die Erstellung einer Datenschutz-Folgenabschätzung. Dies gilt insbesondere dann, wenn es sich um die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DS-GVO) handelt (siehe Punkt 2.6).

Der BfDI hat in einer am 01.03.2013 herausgegebenen „Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“ hierzu einige grundsätzliche Aussagen getroffen, die die SV-Träger beachten sollten.
Nach Auffassung des BfDI unterliegen Gesundheitsdaten dem Schutzbedarf „sehr hoch“[31]. Bei diesen ist eine Ende-zu-Ende-Verschlüsselung (§ 5 Abs. 3 Satz 3 DeMailG) zwingend notwendig. Auch das Bundesinnenministerium (BMI) weist hierauf in seinem „Minikommentar“ zum EGovG ausdrücklich hin.

Für den Schutzbedarf „hoch“ empfiehlt die Aufsicht des Bundesversicherungsamtes bei Abruf von Gesundheitsdaten (z. B. Patientenquittung) aus einem Online-Portal (Online-Geschäftsstelle) heraus eine Authentifizierung basierend auf zwei Faktoren (z. B. Benutzername / Passwort sowie einem weiteren Sicherungsmittel wie z. B. der eID des neuen Personalausweises (nPA) / der elektronischen Gesundheitskarte - siehe Rundschreiben des Bundesversicherungsamtes vom 5. September 2014).

Der GKV-Spitzenverband hat in Abstimmung mit dem BfDI und BSI eine Richtlinie gem. § 217f Abs. 4b SGB V zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme erarbeitet.[32] Die Regelungen der endgültigen Fassung haben die Krankenkassen bei Kontakten mit ihren Versicherten anzuwenden.

Die Prüfdienste empfehlen den SV-Trägern ebenfalls dringend, besondere Vorkehrungen bei der Authentifizierung vorzusehen, z. B eine qualifizierte Zwei-Faktor-Authentifizierung

- Benutzername / Password **und**
- weiteres Sicherungsmittel wie (transaktions- oder zumindest sitzungsbezogenes) TAN-Verfahren oder – alternativ zu TAN-Verfahren - als besonders sicherem weiteren Sicherungsmittel die eGK bzw. den nPA (vgl. Punkt 4.2.3.1 und 4.2.3.5).

Die Prüfdienste empfehlen, diese Vorkehrungen auch bei der Übermittlung sensibler Informationen von Versicherten an den SV-Träger vorzusehen.

Für Apps gelten die dargestellten Anforderungen in gleichem Maße. Dabei ist bei der Festlegung der Anforderungen zwischen den verschiedenen Funktionen und Inhalten von Apps zu unterscheiden:

- Anmeldung in der Online-Geschäftsstelle über die App:
  - Gleiche Schutzklassen / Anforderungen wie bei Online-Portalen
- Informationsaustausch nur über Application-Server (ohne Account bei Online-Portal):
  - Serverbasierte Schutzmaßnahmen in Bezug auf
    - Integrität der App
    - Sicherung der Übertragungswege
  - Gleiche Schutzklassen wie bei Online-Portalen
- Datenabruf vom Server (z. B. allgemeine Informationen ohne personenbezogene Daten:
  - Keine Speicherung von nicht erforderlichen Daten (Zweckbindung, Datensparsamkeit)

Zu den datenschutzrechtlichen Anforderungen an die Erstellung und das Angebot von Apps

[31] Hier ist die Einstufung in die Schutzklasse „sehr hoch“ mit der Sicherheitsstufe „hoch“ nach eIDAS-Verordnung gleichzusetzen (siehe dazu Punkt 4.2.3.1)

[32] Richtlinie zu Maßnahmen zum Schutz von Sozialdaten der Versicherten vor unbefugter Kenntnisnahme nach § 217f Absatz 4b SGB V (GKV-SV Richtlinie Kontakt mit Versicherten) vom 14.12.2018; abrufbar unter: https://www.gkv-spitzenverband.de/media/dokumente/krankenversicherung_1/telematik/sozialdaten/20190206_Richtlinie_217f_Abs4b_SGB_V.pdf

verweisen die Prüfdienste auf die Veröffentlichungen der Datenschutzbehörden[33].

4.2 Zugang / Eröffnung der Kommunikation

4.2.1 Grundsätze

Der Austausch elektronischer Dokumente zwischen Versicherten und SV-Träger wird im § 36a SGB I geregelt. Danach ist die Übermittlung elektronischer Dokumente zulässig, soweit der Empfänger hierfür einen Zugang eröffnet hat.

Für die Kommunikation **SV-Träger → Versicherte** bedeutet dies, dass die Versicherten gegenüber dem SV-Träger ausdrücklich ihre Zustimmung für die Übermittlung elektronischer Dokumente (z. B. per E-Mail) erteilt haben müssen (§ 36a Abs. 1 SGB I). Die bloße Angabe einer E-Mail-Adresse reicht nicht aus.

Dagegen ist für eine Kommunikation in Gegenrichtung **Versicherte → SV-Träger** die Bekanntgabe einer E-Mail-Adresse des SV-Trägers als Zustimmung anzusehen.

Ergänzend wird in § 2 EGovG festgelegt, wie die verschiedenen Zugänge bei den Behörden zu schaffen sind.

- Absatz 1 gibt vor, dass jede Behörde – spätestens seit 01.07.2014 – einen Zugang für die Übermittlung elektronischer Dokumente zu schaffen hat, die auch mit einer QES versehen sind. Eine Festlegung auf ein bestimmtes Verfahren erfolgt hierdurch nicht. Soweit die Behörde ein E-Mail-Postfach hat, kann sie auch qualifiziert signierte elektronische Dokumente empfangen. Neben dem E-Mail-Postfach ist z. B. auch die Einrichtung eines elektronischen Zugangs über Verwaltungspostfächer oder über Online-Formulare und Web-Anwendungen möglich.

  Eine Verpflichtung zur Überprüfung einer Signatur oder zur Annahme von verschlüsselten Dokumenten wird durch das EGovG nicht begründet. Eine solche kann sich jedoch aus anderen gesetzlichen Vorschriften ergeben, z. B. aus § 110a SGB IV i. V. m. Art. 5 und 32 DS-GVO.

- Absatz 2 verpflichtet Behörden des Bundes zusätzlich, ein De-Mail-Konto im Sinne von § 5 De-Mail-Gesetz zu eröffnen. Diese Verpflichtung trifft nur die Bundesbehörden und Körperschaften, die (künftig) einen Zugang zu dem zentral im internen Verbindungsnetz des Bundes geplanten „De-Mail-Gateway“ haben.
  De-Mail-Nachrichten gelten als beim SV-Träger eingegangen, sobald sie sich im De-Mail-Postfach des SV-Trägers beim zugehörigen De-Mail-Diensteanbieter befinden.

  Eine Verpflichtung des SV-Trägers, den Versicherten auf dem De-Mail-Wege zu antworten, besteht nicht, wenn die Versicherten mehrere Zugänge gegenüber dem SV-Träger eröffnet haben. Außerdem ist der SV-Träger nicht verpflichtet, per De-Mail zu antworten. Wenn es sich um Sozialdaten mit sehr hohem Schutzbedarf handelt, sind bei elektronischen Antwor-

[33] Z. B. Entschließung der 91. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Schwerin, 6./7. April 2016): „Wearables und Gesundheits-Apps – Sensible Gesundheitsdaten effektiv schützen!“ sowie Düsseldorfer Kreis der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (16. Juni 2014): „Orientierungshilfe zu den Datenschutzanforderungen an App-Entwickler und App-Anbieter“.

ten zusätzliche Sicherungsmaßnahmen (z. B. Ende-zu-Ende-Verschlüsselung) einzusetzen.

- In Absatz 2 Satz 5 werden die Behörden des Bundes darüber hinaus verpflichtet, in Verwaltungsverfahren, in denen sie aufgrund einer Rechtsvorschrift die Identität der Versicherten festzustellen haben oder aus anderen Gründen eine Identifizierung für notwendig erachten, dies über einen elektronischen Identitätsnachweis nach § 18 Personalausweisgesetz bzw. § 78 Abs. 5 des Aufenthaltsgesetzes anzubieten. Bei gesetzlich Krankenversicherten kann dieser Nachweis auch mit der elektronischen Gesundheitskarte erfolgen (§ 36a Abs. 2 Satz 5 SGB I).

Hinweis:
Nur die Informationen der Versicherten, die über Verfahren gewonnen werden, die die im folgenden genannten Anforderungen an Authentifizierung, Integrität der Daten und revisionssichere Speicherung erfüllen, werden von den Prüfdiensten zu Prüfzwecken als Beleg anerkannt.

Die Anforderungen des Onlinezugangsgesetzes[34] sind in die Überlegungen der SV-Träger zur Gestaltung von Kommunikationsverfahren einzubeziehen. Hiernach sind spätestens bis Ende 2022 grundsätzlich alle Dienstleistungen über die entsprechenden Portale anzubieten und bestehende Portale zu einem Portalverbund zu verknüpfen.

4.2.2 Zugangsmöglichkeiten bei Schriftformersatz

4.2.2.1 Qualifizierte Elektronische Signatur

In § 36a Abs. 2 Satz 1 – 3 SGB I wird geregelt, dass eine durch Rechtsvorschrift angeordnete Schriftform – soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist – durch die elektronische Form ersetzt werden kann. In diesem Fall ist das ausgehende Dokument **vom Absender zwingend** mit einer Qualifizierten Elektronischen Signatur (QES) nach eIDAS-Verordnung / VDG zu versehen. Die Verwendung von Pseudonymen ist hierbei nicht zulässig.

Nähere Erläuterungen zur QES enthält Punkt 3.2.2, zum Schriftformerfordernis siehe Punkt 4.1.2.

4.2.2.2 Eingabe über Web-Formulare oder besondere Eingabegeräte

Eine durch Rechtsvorschrift angeordnete Schriftform kann – neben der Verwendung einer QES – auch „durch unmittelbare Abgabe der Erklärung in einem elektronischen Formular“ ersetzt werden, welches der SV-Träger „in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung stellt“ (§ 36a Abs. 2 Satz 4 Nr. 1 SGB I).

Die Formulierung stellt klar, dass hiermit nicht elektronische Formulare gemeint sind, die die Versicherten über das Internet herunterladen, am Bildschirm ausfüllen (z. B. ausfüllbares PDF-Formular) und anschließend ausdrucken und an den SV-Träger schicken. Die Regelung betrifft die „Direktausfüllung“, also die unmittelbare Eingabe von Daten in eine vom SV-Träger zur Verfügung gestellte unveränderbare elektronische Maske (Formular). Die Eingabe kann erfolgen

[34] Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen, BGBl. I 2017, S. 3138.

über Web-Anwendungen oder in vom SV-Träger zur Verfügung gestellten Eingabegeräten (z. B. in seinen Kundenzentren)[35]. Die elektronische Anwendung fungiert wie ein Formular, das aus der Ferne ausgefüllt wird.

Empfehlung: Der SV-Träger sollte durch die technische Ausgestaltung der zur Verfügung gestellten Anwendung und die eröffneten Auswahl- oder Ausfüllfelder selbst steuern, welche Erklärungen abgegeben werden können.

Die Versicherten müssen sich zur Nutzung identifizieren (Authentifizierung). Dies kann (gem. § 36a Abs. 2 Satz 5 SGB I) über die eID-Funktion des neuen Personalausweises (nPA) bzw. des elektronischen Aufenthaltstitels (eAT) oder die elektronische Gesundheitskarte (eGK) erfolgen. Der SV-Träger hat dabei insbesondere sicherzustellen, dass die von Versicherten eingegebenen Erklärungen (Daten) mit den Identifikationsdaten des nPA / der eGK („Metadaten", z. B. Personalausweisdaten, Eingabezeit) dauerhaft verknüpft werden. Abgeleitet aus § 110a SGB IV i. V. m. Artikeln 5 und 32 DS-GVO sind diese Daten revisionssicher zu speichern.

Die technische und organisatorische Ausgestaltung des Gesamtverfahrens (von der Eingabe durch die Versicherten bis zur Übergabe der Daten an die Fachanwendung und das Langzeitarchiv) ist in einer ausführlichen Verfahrensbeschreibung zu dokumentieren. Hierzu gehört auch die Beschreibung des Verfahrens zum Auslesen der über die Web-Anwendung eingegangenen Daten / Dokumente (einschließlich Metadaten).

In der Verfahrensbeschreibung sind insbesondere die erforderlichen technischen Sicherheitsstandards zu beschreiben. Der SV-Träger hat hierbei u.a. die datenschutzrechtlichen Vorschriften sowie die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgestellten Grundsätze zur Datensicherheit zu beachten.

4.2.2.3 Kommunikation mit De-Mail

Nach § 36a Abs. 2 Satz 4 Nr. 2 SGB I kann eine durch Rechtsvorschrift angeordnete Schriftform auch durch Versendung eines elektronischen Dokuments an den Versicherungsträger mit der **Versandart nach § 5 Abs. 5 DeMailG** ersetzt werden.

Der akkreditierte De-Mail-Diensteanbieter muss danach dem Nutzer ermöglichen, seine „**sichere Anmeldung**" im Sinne von § 4 DeMailG in der Nachricht so bestätigen zu lassen, dass die Unverfälschtheit der Bestätigung jederzeit nachprüfbar ist. Um dieses dem Empfänger der Nachricht kenntlich zu machen, bestätigt der akkreditierte De-Mail-Diensteanbieter des Senders die Verwendung der sicheren Anmeldung nach § 4 durch eine QES.

Der akkreditierte De-Mail-Diensteanbieter hat zu gewährleisten, dass der Nutzer (Absender) zwischen mindestens zwei Verfahren zur sicheren Anmeldung wählen kann. Ein Verfahren muss hierbei die Nutzung der eID-Funktion des neuen Personalausweises (nPA) ermöglichen (§ 4 Abs. 2 DeMailG).

Das bedeutet:

- Bei einem bestehenden **Schriftformerfordernis** muss sich der Absender an seinem De-Mail-Konto „sicher angemeldet" haben. Hierzu muss er für die Anmeldung zwei geeignete

[35] Eine (teilweise/vollständig) kostenlose Überlassung von elektronischen Eingabegeräten (z. B. Kartenleser) für Versicherte **durch den SV-Träger** ist gem. § 30 Abs. 1 SGB IV nicht zulässig!

und voneinander unabhängige Sicherungsmittel einsetzen.
Dies können sein:

1. Sicherungsmittel = Benutzername und Passwort (mit weiterem Sicherungsmittel PIN)
2. Sicherungsmittel = eID-Funktion des nPA

Hierzu muss der Absender über die für die Nutzung der eID-Funktion des nPA erforderliche technische Ausstattung (Kartenlesegerät) und einen hierzu geeigneten Browser verfügen.

- Der De-Mail-Diensteanbieter des Absenders muss in den Metadaten der Nachricht bestätigen, dass der Absender die sichere Anmeldung gem. § 5 Abs. 5 DeMailG gewählt hat. Diese Wahl muss aus der gesendeten Mail in der Form, wie sie beim Empfänger angekommen ist, dauerhaft erkennbar sein.

- Die mit der Versandoption „absenderbestätigt" versendete De-Mail wird automatisch mit einer QES versehen. Diese wird nicht durch den Absender selbst, sondern seinen De-Mail-Diensteanbieter angebracht. Die QES muss die Nachricht selbst, alle angehängten Dateien und die Metadaten umfassen. Durch die QES wird bestätigt, dass die Nachricht des Absenders mit diesem Inhalt versandt wurde. Der Empfänger der Nachricht muss diese einschließlich der Metadaten und der QES archivieren. Die Form der Signierung bleibt hierbei nur solange erhalten, wie das Dokument mit der jeweiligen De-Mail-Nachricht verbunden bleibt. Die Nachricht sowie ihre Anhänge können nach dem Versand nicht unerkannt verändert werden (Integritätsschutz).

- Um die Nachprüfbarkeit der Signatur zu erhalten, dürfen auf der Empfängerseite die Nachricht und die Anhänge (z. B. PDF-Dokumente) nicht getrennt werden, sondern müssen als Ganzes aufbewahrt werden.

- Für die QES dürfen ausschließlich Zertifikate von qualifizierten Vertrauensdiensteanbietern verwendet werden. Nur diese bieten die Gewähr, dass die Signaturen dauerhaft überprüfbar bleiben.

4.2.2.4 De-Mail-Versand elektronischer Verwaltungsakte oder sonstiger elektronischer Dokumente durch SV-Träger

Nach § 36a Abs. 2 Satz 4 Nr. 3 SGB I können SV-Träger elektronische Verwaltungsakte oder sonstige elektronische Dokumente – sofern ein gesetzlich festgelegtes Schriftformerfordernis besteht – als De-Mail-Nachricht mit der Versandoption „absenderbestätigt" (gem. § 5 Abs. 5 DeMailG) versenden.

Hierbei muss der De-Mail-Diensteanbieter bei seiner in der Nachricht mitzusendenden Bestätigung (der sicheren Anmeldung) auch den erlassenden SV-Träger als Nutzer erkennen lassen. Beide Daten sind als Metadaten Bestandteil der Nachricht.

4.2.2.5 Identifizierung des Absenders durch sonstige sichere Verfahren

Der Gesetzgeber hat in § 36a Abs. 2 Satz 4 Nr. 4 SGB I festgelegt, dass auch andere sichere Verfahren die Authentizität des Datenübermittlers (Absender der Daten) und die Integrität des elektronisch übermittelten Datensatzes (Inhalt) sowie die Barrierefreiheit gewährleisten können. Derartige Verfahren können nur über eine Rechtsverordnung festgelegt werden, die durch die Bundesregierung – mit Zustimmung des Bundesrates – erlassen wird.

4.2.3 Zugangsmöglichkeiten ohne Schriftformerfordernis

Auch bei Dokumenten, für die kein Schriftformerfordernis gesetzlich festgelegt ist, kann eine Übermittlung an den SV-Träger über die vorgenannten Zugangsmöglichkeiten (Web-Portal, De-Mail) erfolgen. In diesen Fällen ist jedoch grundsätzlich keine Authentifizierung über die in § 36a Abs. 2 Satz 4 SGB I genannten Zugangsmöglichkeiten erforderlich.

Gleichwohl kann es erforderlich sein, dass die Authentizität des Absenders und die Integrität der Originaldaten und deren revisionssichere Speicherung aus anderen Gründen (z. B. für RSA-Prüfungen) nachzuweisen sind. Sollten für diese Daten die in § 36a Abs. 2 SGB I genannten sicheren Zugangsmöglichkeiten nicht angewandt werden, muss der Nachweis der Authentizität und Integrität der Daten / Dokumente auf andere Weise erbracht werden. Das gesamte beim SV-Träger zur Anwendung kommende Verfahren ist in einer Verfahrensbeschreibung detailliert zu dokumentieren.

4.2.3.1 Authentifizierungsverfahren - Allgemein

Zur Anerkennung von elektronisch übermittelten Daten ist die Identität des Absenders über ein Authentifizierungsverfahren festzustellen.

Schutzbedarfsfeststellung:
Bevor eine Entscheidung über die Art der Authentifizierung getroffen wird, hat der SV-Träger im Rahmen einer Schutzbedarfsanalyse festzulegen, welche Daten über das Online-Portal übermittelt bzw. abgerufen werden können.

- Hierbei können insbesondere die Ausführungen des BfDI („Handreichung zum datenschutzgerechten Umgang mit besonders schützenswerten Daten beim Versand mittels De-Mail“) im Hinblick auf die Übermittlung von Sozial- und Gesundheitsdaten als allgemein zu verstehende Anforderungen an die Schutzbedarfsfeststellung herangezogen werden. Dies bedeutet, dass je nach Schutzbedarf innerhalb des Portals ggf. zusätzliche Authentifizierungen für den Abruf „besonders schützenswerter“ Daten einzurichten sind.
- Zur Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen kann auch die TR-03147 herangezogen werden, die die Bedrohungen und Anforderungen für Verfahren zum Identitätsnachweis und zur Identitätsprüfung natürlicher Personen betrachtet.

Aus der Schutzbedarfsanalyse ergibt sich die Einstufung der elektronisch übermittelten bzw. zu übermittelnden Daten in die Sicherheitskategorien „normal“, „substanziell“ und „hoch“.[36]

> Hinweis: In der bisherigen Version des Leitfadens wurden die Kategorien normal / hoch / sehr hoch verwandt. Diese entsprechen nunmehr den Kategorien normal / substanziell / hoch, um eine einheitliche Begrifflichkeit mit der eIDAS-Verordnung und der TR-03147 herzustellen.

Der Schutzbedarf wird in der Regel getrennt nach verschiedenen Schutzzielen betrachtet. Im weiteren Verlauf werden nur die Schutzziele Vertraulichkeit, Integrität und Nichtabstreitbarkeit behandelt.

[36] Die verwendeten Kategorien entsprechen denen der TR-03147 bzw. der eIDAS-Verordnung. Die eIDAS-Verordnung verwendet für die unterste Kategorie die Bezeichnung „niedrig“. Es wird an dieser Stelle jedoch die Begrifflichkeit „normal“ verwendet, die auch in der TR-03147 überwiegend verwandt wird.

Hinweise zur Klassifizierung von elektronischer Eingangspost bzw. der Anzeige von Informationen innerhalb eines Online-Portals enthalten die Technische Richtlinie des BSI („TR-03138 TR-RESISCAN“) sowie das „Organisationskonzept elektronische Verwaltungsarbeit“ des Bundesministeriums des Innern. In diesen Dokumenten erfolgt die Klassifizierung des Schutzbedarfs in drei Stufen.

Je nach Schutzbedarfseinstufung der elektronischen Daten im Online-Portal oder bei der Übermittlung von Informationen ist auch das Authentifizierungsverfahren für die Nutzung einer Online-Geschäftsstelle oder App durch die Versicherten zu gestalten und einzurichten. Die nachfolgende Übersicht enthält einen groben Rahmen der Maßnahmen zu den jeweiligen Schutzbedarfen:

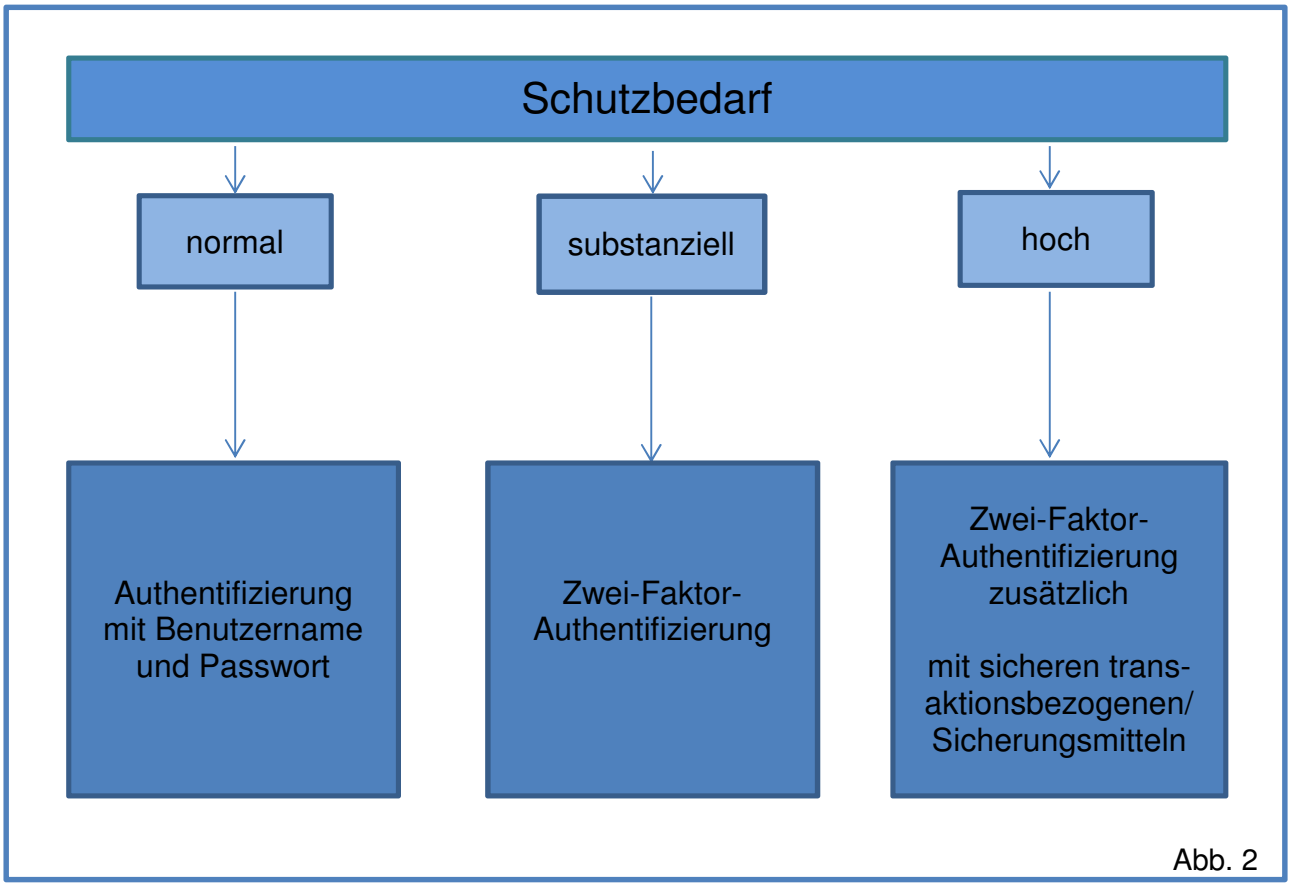


Abb. 2

4.2.3.2 Anforderungen an Authentifizierung

a) Die **Mindest- oder Basisanforderung der Prüfdienste** für eine Authentifizierung für die Übermittlung von individuellen Informationen (persönliche individualisierte Daten), die nicht öffentlich-allgemein abrufbar sind, ist die Zwei-Faktor-Authentifizierung. Dabei enthält die Zwei-Faktor-Authentifizierung eine Kombination zweier unterschiedlicher unabhängiger Kanäle / Faktoren, die zusammen für den Identitätsnachweis eingesetzt werden.
Zu den zwei Faktoren der Authentifizierung gehören z. B. der elektronische und postalische Weg und zu den Faktoren „Besitz“ (mit Biometrie), „Wissen“.

So kann mit der Abfrage des Identifikationsmerkmals „Nutzername und Passwort“ (der Nutzername bietet erst zusammen mit dem zugehörigen Passwort die Authentifizierung) nur die Sicherheit für einen normalen Schutzbedarf erreicht werden, da der Nutzername das einzige Iden-

titätsattribut darstellt. Die statischen Identifikationsmerkmale bieten – unabhängig von deren Zustellverfahren / Erstregistrierung (siehe d) - (alleine) keinen ausreichenden Schutz für einen höheren Schutzbedarf.

b) Eine **höhere Sicherheit (substanzieller / hoher Schutzbedarf)** kann nur erreicht werden, wenn zusätzliche Geheimnisse wie z. B. PIN und weitere Authentifizierungsfaktoren (z. B. über Softwaretoken, Hardwaretoken) sowie kryptographische Sicherungsverfahren genutzt werden.[37] Dabei werden im Rahmen einer sich verändernden Authentifizierungsgrundlage[38] in der Regel kryptographische Mechanismen eingesetzt, so dass sich die zum Nachweis der Identität anzugebenden Daten bei jedem Authentifizierungsvorgang ändern.

Dabei ist von einer sicheren bzw. „starken" Authentifizierung auszugehen, wenn zusätzlich zu Elementen der Authentifizierung mindestens zwei unabhängige Faktoren eingesetzt werden.[39]

So sind für den Schutzbedarf „hoch" transaktionsbezogene bzw. sitzungsbezogene Sicherungsmittel in sicherer Ausgestaltung in den Authentifizierungsverfahren zusätzlich zu integrieren.

Die „Zusatz-Authentifizierung" muss bei jeder Transaktion besonders schützenswerter Daten erneut erfolgen. Eine dauerhafte Freischaltung durch einmalige Eingabe dieser „Zusatz-Authentifizierung" ist nicht zulässig.

Um die Authentizität / Integrität / Vertraulichkeit der Identifikationsmerkmale während der Übermittlung zu schützen, muss vor der Übermittlung eine zwischen der Person, dem Portal und dem zusätzlichen Authentifizierungsgerät sichere Verbindung etabliert werden.
Werden Dienste über öffentliche Netze bereitgestellt, so müssen Verfahren implementiert werden, die es den Nutzern ermöglichen, die Identität des Anbieters/SV-Trägers zu verifizieren („sichere Verbindung"). Bei Web-Anwendungen kommt dazu regelmäßig eine zertifikatsbasierte Authentifizierung über TLS zum Einsatz.

Weiterhin sind die Identifikationsmerkmale durch Verschlüsselungstechniken vor unbefugtem Zugriff zu schützen, da sie bereits selbst schutzwürdige Daten enthalten können.

Hieraus kann beispielhaft abgeleitet werden:

- Die Anzeige einer „Patientenquittung" (§ 305 SGB V) innerhalb eines Online-Portals ist – aufgrund der darin enthaltenen Gesundheitsdaten – zweifelsfrei dem Schutzbedarf „hoch" zuzuordnen.
- Für den Schutzbedarf „hoch" empfiehlt die Aufsicht des Bundesversicherungsamtes aus einem Online-Portal (Online-Geschäftsstelle) heraus eine Authentifizierung basierend auf zwei Faktoren, z. B. Benutzername / Passwort sowie einem weiteren Sicherungsmittel wie z. B. der eID des nPA / der eGK[40] .

[37] Zu „technischen" Hinweisen siehe z. B. die Ausgabe 4/2016 der Zeitschrift „Datenschutz und Datensicherheit" (DuD).

[38] Im Gegensatz dazu wird unter dem Begriff „dynamische Authentifizierung" verstanden, dass die Authentifizierungstechniken abhängig von Kontext und Vorgang geändert werden (z. B. nur ein Faktor bei Login aus gesichertem Firmennetz, aber mehrere, wenn Zugriff von einem öffentlichen Hotspot aus erfolgt). Dies kann ebenfalls in einem Authentifizierungskonzept berücksichtigt werden.

[39] Siehe Art. 8 Verordnung (EU) Nr. 910 / 2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG – sog. e-IDAS-Verordnung: Sicherheitsniveau substanziell.

[40] Rundschreiben des Bundesversicherungsamt vom 05.09.2014 zur Sicherung des Online-Portals vor unberechtigten Zugängen und zur Verhinderung unbefugter Zugriffe auf Patientendaten im Rahmen der Patientenquittung gem. § 305 Abs. 1 SGB V sowie Rundschreiben vom 18.04.2016 zum Zugangs- und Zugriffsschutz bei digitalen Anwendungen.

- Die einmalige Authentifizierung am Online-Portal (Benutzername / Passwort) reicht nach Auffassung auch der Prüfdienste in keinem Fall für eine Anzeige derartiger Daten aus. Die Prüfdienste empfehlen daher ebenfalls dringend, besondere Vorkehrungen bei der Authentifizierung (qualifizierte Zwei-Faktor-Authentifizierung) vorzusehen:
  - Anmeldung mit Nutzername / Passwort **und** einem weiteren (transaktionsbezogenen oder zumindest sitzungsbezogenen) Sicherungsmittel, das mindestens z. B. ein TAN-Verfahren darstellt bzw. – als höhere Sicherheitsstufe – die Nutzung nPA / eGK.

Änderungen sensibler Stammdaten (Adressänderungen, Bankverbindungen etc.) sind nach Auffassung der Prüfdienste ebenfalls dem Schutzbedarf „hoch“ zuzuordnen.
Die Prüfdienste empfehlen dringend, Änderungen dieser Daten durch Versicherte über elektronische Kommunikation ebenfalls erst nach einer zusätzlichen Authentifizierung vorzusehen. Hierzu kann auch ggf. das mTAN-Verfahren (wie im Bankensektor üblich) genutzt werden.

c) Eine Authentifizierung oder Übermittlung / Änderung eines Geheimnisses als Sicherungsmittel über **Telefon** (Telefonzentrale) für eine anschließende Datenübermittlung sollte nicht (Empfehlung der Prüfdienste) bzw. nur bei weiterer, sicherer / zweifelsfreier Identifizierung der/des Versicherten im Rahmen des Telefonkontaktes erfolgen.[41]

d) **Modularer Aufbau und Wirkung**
Die Prüfdienste empfehlen, ein Konzept zu Authentifizierungslösungen zu erstellen, in das die zu übermittelten / erhaltenen Informationen, deren Schutzbedarf und Authentifizierungslösungen für die einzelnen Sachverhalte aufgegriffen und Authentifizierungsmodule dargestellt werden.

Neben der Erstaufstellung sollte auch ein Verfahren zur regelmäßigen Weiterentwicklung implementiert werden.

Ein Konzept zu Authentifizierungslösungen, das die verschiedenen Schutzbedarfe berücksichtigen muss, kann modular aufgebaut sein und Module aufeinander aufbauend verbinden:

- Erstidentifikation / Erst-Authentifizierung[42]:
  Bei der Erstidentifikation können verschiedene Möglichkeiten vorgesehen werden, die wiederum unterschiedlichen „Sicherheitsklassen“ (entsprechend Schutzbedarf) entsprechen können.
  Zu nennen sind z. B.
  - siehe Punkt 4.2.3.3 zur Eröffnung eines dauerhaften Zugangs
  - Identifizierungsverfahren nach BPersAG (siehe unten)

- Transaktions- oder sitzungsbezogene Authentifizierungsmittel[43]:
  Auch hierbei können Authentifizierungsmittel für unterschiedliche „Sicherheitsklassen“ vorgesehen werden, die mit steigender Sicherheit auch Zwei-Faktoren-Authentifizierungsmittel darstellen
  - TAN-Verfahren
  - TAN-Verfahren mit Nutzung weiterer sicherer Geheimnisse (z. B. zugesandte mTAN und zusätzlich eine Ziffernfolge der eGK-Kartennummer)
  - Zusendung der mTAN an ein Gerät, durch das nicht die Anforderung der mTAN erfolg-

[41] Rundschreiben des Bundesversicherungsamtes vom 18.04.2016 zum Zugangs- und Zugriffsschutz bei digitalen Anwendungen

[42] Im Sinne Verknüpfung eines „Accounts“ mit einer Person / Versicherten.

[43] Authentifizierungen, die den Zugang für die Dauer der Kommunikation („Sitzung“) bzw. für eine Handlung („Transaktion“) ermöglichen.

te (bei mobiler Kommunikation)
- Weitere Verfahren, die außerhalb des mTAN-Verfahrens ein weiteres Geheimnis liefern (z. B. Zugangstoken, biometrische Faktoren)
- Nutzung eID-Funktionen insbesondere der eGK

Mit dem Gesetz zur Förderung des elektronischen Identitätsnachweises[44] werden mit der Ergänzung des Bundespersonalausweisgesetzes erweiterte Nutzungsmöglichkeiten der eID Funktion des Bundespersonalausweises geschaffen. Der Bereich der Anwendungsmöglichkeiten wird dadurch über die bisherigen Möglichkeiten (z. B. Eröffnung eines Bankkontos) hinaus erweitert. Identifizierungsdienstleister (siehe § 2 Abs. 3a BPersAG n.F.) können Bestätigungen der Identität von Personen für Kunden vornehmen. Die so verifizierten Daten von Personen können dann von den Kunden (z. B. SV-Trägern) für die Authentifizierung genutzt werden (§ 19a BPersAG n.F.)
Im Rahmen der Wirtschaftlichkeitsbetrachtung sollte eingehend geprüft werden, für welche Module diese neuen Möglichkeiten bei ggf. fallzahlenmäßiger Abrechnung der Identifizierungsdienstleister genutzt werden (z. B. nur für die sichere Erstregistrierung).

Auch wenn die Authentifizierungsfunktionen der eGK derzeit nur über die entsprechende (Telematik-)Infrastruktur einsetzbar sind, sollten konzeptionelle Überlegungen die eGK als sehr sicheres Authentifizierungsmittel bereits berücksichtigen.
Das BMG prüft derzeit die Einführung alternativer Authentifizierungswege für die Telematikinfrastruktur.

Die jeweiligen Bausteine der Erstidentifikation und der weiteren (transaktions-/sitzungsbezogenen) Identifikationsmaßnahmen sind in ihrer konkreten Schutzwirkung grundsätzlich gesondert zu betrachten.
Eine Zwei-Faktor-Authentifizierung bei der Erstregistratur reicht in ihrer Wirkung nicht über das Verfahren der Erstregistratur als (grundsätzlicher) Verknüpfung der Authentifizierung mit der natürlichen Person hinaus.

Bei substanziellem / hohem Schutzniveau ist daher auch die Verknüpfung zur natürlichen Person transaktions- oder sitzungsbezogen sicher und ggf. auch im Wege einer (weiteren) Zwei-Faktor-Authentifizierung (dann transaktions-/sitzungsbezogen) festzustellen.

Dies bedeutet, je sicherer die Erstregistrierung und darüber hinaus weitere Authentifizierungsmittel bereits jeweils für sich und ihre Zwecke sind, desto sicherer ist die Kombination bzw. der modulare Aufbau bei deren kumulativer Verwendung für die entsprechende Gesamthandlung, für die die Authentifizierung erfolgt.

Bei einer Lösung, die über einen (ggf. kassenexternen) Zugang die Authentifizierung für mehrere Kassenanwendungen ermöglichen soll (sog. Single Sign-on oder SSO) reicht der Schutzbereich dieser SSO-Lösung nur insoweit, wie die Schutzbereiche / Schutzbedarfe der jeweiligen Authentifizierungsmaßnahmen dieses Punktes reichen. Auf diesen Schutzbereich kann dann jedoch durch weitere Maßnahmen aufgebaut werden.

4.2.3.3 Eröffnung eines dauerhaften Online-Zugangs („Benutzer-Konto“)

Der Antrag auf Eröffnung eines Zugangs zum Online-Portal („Online-Geschäftsstelle“) kann schriftlich oder über eine Web-Anwendung erfolgen. **Die Mindestanforderung der Prüfdienste**

[44] Gesetz zur Förderung des elektronischen Identitätsnachweises vom 07. Juli 2017, BGBl 2017 I, S. 2310.

ist eine Zwei-Faktor-Authentifizierung. Die Beantragung kann folgendermaßen ausgestaltet werden:

Von den Versicherten sind bestimmte Daten zur „Erstidentifikation“ (Registrierung) abzufordern. Hierzu gehören mindestens:

- Name, Vorname
- Geburtsdatum
- eindeutiges Identifizierungsmerkmal, z. B. KV-Nummer (Sicherer wäre z. B. die Abfrage von Teilen der eGK-Kartenkennnummer (ICCSN))

Optional können an dieser Stelle bereits auch schon folgende Daten (für die spätere Nutzung des Online-Portals) von den Nutzern eingegeben werden, z. B.:

- Benutzername
- Passwort
- E-Mail-Adresse
- Mobilfunknummer

Nach Absendung der Daten erfolgt ein Abgleich der eingegebenen Mindestdaten mit den im Bestand des SV-Trägers vorhandenen Daten. Die optional bereits angegebene E-Mail- Adresse kann - nach Abgleich mit den beim SV-Träger ggf. bereits bekannten Daten - durch Zusendung einer E-Mail mit einem „Verifizierungslink“ geprüft werden.

Nach Annahme und Verifizierung der Daten durch den SV-Träger hat dieser dem Nutzer einen **Freischaltcode** postalisch zuzustellen. Dieser Freischaltcode ist vom Nutzer innerhalb einer vom SV-Träger festzulegenden Gültigkeitsdauer (maximal 60 Tage) bei der Erstanmeldung im Online-Portal einzugeben. Hierdurch wird das Online-Portal für Geschäftsprozesse des normalen Schutzbedarfs freigeschaltet.
Entsprechend den festgelegten datenschutzrechtlichen Sicherheitsanforderungen kann innerhalb des Online-Portals eine zusätzliche Authentifizierungsabfrage für „höherwertige“ Geschäftsprozesse notwendig werden (vgl. Punkt 4.2.3.2).

Die SV-Träger dürfen nur eine einmalige Nutzung des Freischaltcode zulassen. Lässt der Nutzer die Frist zur Ersteingabe verstreichen, muss er einen neuen Freischaltcode vom SV-Träger anfordern.

Die SV-Träger haben die technischen Voraussetzungen dafür zu schaffen, dass sowohl der von ihnen zu vergebene **Freischaltcode** als auch das vom Nutzer festzulegende **Passwort** für den Online-Zugang die in den IT-Grundschutzkatalogen des BSI enthaltenen Vorgaben erfüllen[45], zumindest:

- Mindestlänge (8 Zeichen)
- Kombination aus Buchstaben, Ziffern und Sonderzeichen
- Keine trivialen Namen / Ziffernkombinationen

Passworte, die diese Kriterien nicht erfüllen, müssen bei der Eingabe/Änderung (online) abgewiesen werden.

Der SV-Träger hat ferner festzulegen, nach wieviel Fehleingaben des Passwortes der Zugang

[45] Siehe z. B.: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html

zum Online-Portal für diesen Nutzer gesperrt wird. Üblich sind hier maximal fünf Versuche.

Bei Übermittlung von Daten der Schutzklasse „substanziell“ oder „hoch“ sollen weitere (transaktionsbezogene / sitzungsbezogene) Sicherungsmittel hinzukommen (siehe Punkt 4.2.3.2).

4.2.3.3.1 Nutzung der biometrischen Daten

Anstatt eines Passworts (mit den o. g. Anforderungen), das vom Nutzer festgelegt wird, können auch biometrische Daten des Nutzers für den dauerhaften Zugang zu einem Online-Portal genutzt werden.

Vor der Einführung eines elektronischen biometrischen Verfahrens soll eine Risikoanalyse aufgrund des Schutzbedarfs der im Online-Portal übermittelten oder gespeicherten personenbezogenen Daten vom SV-Träger durchgeführt werden.

Weiterhin soll das biometrische Verfahren folgenden Anforderungen genügen:

- Die aufgenommenen biometrischen Daten / Merkmale sollen lokal (auf dem Smartphone oder Rechner des Nutzers) in einem gesicherten Bereich kryptographisch verschlüsselt und gespeichert werden. Der SV-Träger darf auf die biometrischen Merkmale des Nutzers nicht zugreifen.
- Bei der Aufnahme von biometrischen Daten müssen typische Merkmale eines langfristig stabilen physiologischen Charakteristikums (z. B. sog. Minuzien der Papillarleisten bei einem Fingerabdruck) für die spätere Verifikation extrahiert werden. Ein einfaches digitales Bild des Körpermerkmals ist für eine Verifikation nicht ausreichend.
- Zusätzlich zum biometrischen Abgleich muss eine Lebenderkennung bei jeder Anmeldung durchgeführt werden. Der Life-Test soll erkennen, ob die jeweiligen biometrischen Merkmale von einer lebenden Person und nicht von einer Kopie oder einem Abbild stammen.
- Neben der Anmeldung mittels eines biometrischen Charakteristikums soll auch eine Anmeldungsmöglichkeit mit einem Passwort (wie in 4.2.3.3 beschrieben) geschaffen werden. Bei mehrmals fehlgeschlagener Anmeldung (max. 5 Fehlversuche) mit einem biometrischen Charakteristikum soll weiter nur die Möglichkeit der Anmeldung mit dem Passwort bestehen. Nach den weiteren fehlgeschlagenen Versuchen (max. 5) bei der Anmeldung mit dem Passwort soll der Zugang zum Online-Portal gesperrt werden.

4.2.3.3.2 Video-Ident-Verfahren

Eine (Erst-)Authentifizierung / Identifizierung für die Eröffnung des Zugangs in einem Online-Portal kann mit Hilfe eines Video-Ident-Verfahrens erfolgen.
Eine Video-Ident-Authentifizierung kann als Grundlage eines Zugangs zu einem Online-Portal mit Daten, die den Schutzbedarf „hoch“ aufweisen, genutzt werden.
Für eine sichere Erstregistrierung sollten folgende Anforderungen / Richtlinien erfüllt werden:[46]

- Das Verfahren muss in Echtzeit und ohne Unterbrechung erfolgen. In Bezug auf Integrität und Vertraulichkeit ist für die Kommunikation nur eine Ende-zu-Ende-Verschlüsselung zulässig.
- Die zu identifizierende Person hat zu Beginn einer Videoauthentifizierung / Video-Identitätsprüfung ihr ausdrückliches Einverständnis damit zu erklären, dass der gesamte

[46] Durch die BaFin zertifizierte Video-Ident-Verfahren sind als sehr sicher einzustufen.

Identifizierungsprozess sowie Fotos bzw. Screenshots ihrer Person und ihres Ausweisdokuments aufgezeichnet werden.

- Eine Videoauthentifizierung darf nur von entsprechend geschulten und hierfür ausgebildeten Beschäftigten durchgeführt werden. Zu den akzeptierten Dokumenten, ihren prüfbaren Merkmalen und den entsprechenden Schulungsmaßnahmen muss eine geeignete Dokumentation vorliegen. Die Schulungen der Beschäftigten müssen in regelmäßigen Abständen (mindestens aber einmal jährlich) sowie bei Bedarf von einem Dritten vorgenommen werden. Ein Bedarf kann z. B. in einer Änderung der gesetzlichen und / oder aufsichtsrechtlichen bzw. datenschutzrechtlichen Anforderungen oder im Falle eines Auftretens einer signifikanten Zahl von Betrugsversuchen, des Bekanntwerdens neuer Betrugsmöglichkeiten oder sonstigen Fehlern im Verfahrensablauf begründet sein.
- Die Beschäftigten müssen sich während der Identifizierung in abgetrennten Räumen und mit einer Zugangskontrolle ausgestatteten Räumlichkeiten befinden.
- Nur Ausweisdokumente, die ausreichend fälschungssichere, im Weißlicht visuell und bei Bildübertragung mittels verfügbarer Technik ausreichend deutlich erkennbare und damit prüfbare Sicherheitsmerkmale sowie über einen maschinenlesbaren Bereich verfügen, können für die Identitätsprüfung im Rahmen eines Videoauthentifizierungsverfahrens / Video-Identitätsprüfung herangezogen werden.
- Für eine zweifelsfreie Identifizierung muss die Bild- und Tonqualität der Kommunikation in einem ausreichenden Maße gegeben sein. Ist das nicht der Fall, so muss das Video-Ident-Verfahren abgebrochen werden.
- Während einer Video-Sitzung müssen drei von insgesamt vier verschiedenen Sicherheitsmerkmalen aus verschiedenen Kategorien überprüft werden.

  Zu den optischen Sicherheitsmerkmalen (in vier Kategorien aufgeteilt) zählen:

  1. beugungsoptisch wirksame Merkmale (holografische Sicherheitsmerkmale / Identigram, Hologramme, Kinematische Strukturen)
  2. Personalisierungstechnik (Laserkippbilder, Ausfüllschrift)
  3. Material (personalisierter Sicherheitsfaden, optisch variable Farben)
     Sicherheitsdruck (Mikroschrift, Guillochen-Struktur)

  Personaldokumente mit weniger Sicherheitsmerkmalen sind von dem Video-Ident-Verfahren ausgeschlossen.
- Im Rahmen des Videoauthentifizierungsverfahrens ist eine Gültigkeits- und Plausibilitätsprüfung der auf dem Ausweis enthaltenen Daten und Angaben vorzunehmen. Dies beinhaltet u. a. die Überprüfung, ob Ausstellungsdatum und Gültigkeitsdatum des Ausweisdokumentes zueinander passen.
- Ein Bestandteil der Überprüfung ist zudem eine automatisierte Berechnung der in der maschinenlesbaren Zone enthaltenen Prüfziffern sowie ein Kreuzvergleich der in ihr enthaltenen Angaben mit den Angaben im Sichtfeld des Ausweisdokumentes. Außerdem ist die Korrektheit von Ziffernorthographie, Behördenkennziffer und der verwendeten Schriftarten zu überprüfen.
- Für die Speicherung der personenbezogenen Daten bei einem Video-Ident-Verfahren gelten folgende Anforderungen des PAuswG:

  - Speicherung der Daten des Personalausweises nur in gesetzlich zulässigen Sachverhalten.
  - Speicherung der Daten durch Dienstleister, die zu Identifizierung innerhalb des Kassenverfahrens erforderlich sind.
  - Übermittlung nur der Daten an den SV-Träger, die im Trägerverfahren zur Identitätsfeststellung im Trägerverfahren erforderlich sind bzw. ggf. für die Abrechnungszwecke benötigt werden.
  - Löschung etwaiger erstellter Kopien / Ablichtungen / Screenshots / Videos des Personalausweises / personenbezogener Daten nach erfolgreicher Identifizierung der Person

beim Dienstleister.

- Die zu identifizierende Person muss während der Videoübertragung eine eigens für diesen Zweck gültige, zentral generierte und von den Beschäftigten an sie (per Post, per E-Mail oder SMS[47]) übermittelte TAN unmittelbar online eingegeben und an den Mitarbeiter elektronisch zurücksenden. Nach einem erfolgreichen systemseitigen Abgleich der TAN ist das Identifizierungsverfahren abgeschlossen.
- Aufstellung eines Schutz-Clusters (Schutzmaßnahmen) zum Video-Ident-Verfahren bzw. den verschiedenen Sicherungsmechanismen innerhalb des Verfahrens. Die Möglichkeit des Vier-Augen-Prinzips bei der Prüfung der Ausweisdokumente muss vorhanden sein. Die Aufnahmen müssen im Authentifizierungsprozess stichprobeartig geprüft werden.

Erfüllen Lösungen nicht alle o.g. Anforderungen, so ist im weiteren Verfahren der Authentifizierung (transaktions- oder sitzungsbezogen) durch ergänzende, kompensierende Maßnahmen sicherzustellen, dass eine ausreichende Absicherung gewährleistet wird.

Nach einer erfolgreichen Identifizierung müssen die vom Authentifizierungsdienstleister erhobenen authentifizierungsrelevanten Daten sicher an den SV-Träger übermittelt und verglichen werden. Nach einem erfolgreichen Matching der Authentifizierungsdaten mit den Bestandsdaten des SV-Trägers soll der Zugang zum Online-Portal eröffnet werden.

Zusätzlich müssen folgende datenschutzrechtliche Anforderungen an die Trägerverfahren gelten:

- Speicherung nur der Daten aus dem Identifizierungsprozess beim SV-Träger, die für die Identifizierung und den Nachweis der sicheren, erfolgreichen Authentifizierung sowie ggf. für die Abrechnungszwecke erforderlich sind.
- Speicherung des Merkmals im Rahmen des Registrierungsprozesses mit den bestätigten Identitätsdaten, auf welchem Wege der Authentifizierung / Feststellung der Identität erfolgt ist.

Das gesamte Verfahren des SV-Trägers soll auch unter den wirtschaftlichen Aspekten gestaltet werden. So soll das Video-Ident-Verfahren ggf. nur für die sichere Registrierung bei einem Online-Portal mit personenbezogenen Daten, die einen hohen Schutzbedarf haben, eingesetzt werden. Zu dem Video-Ident-Verfahren sollen zusätzlich andere Möglichkeiten der sicheren Authentifizierung vom SV-Träger angeboten werden.

4.2.3.4 „Einmal-Kennwort-Verfahren“

Für Versicherte, die den vollen Funktionsumfang einer Online-Geschäftsstelle (noch) nicht nutzen, aber z. B. bei einzelnen Fragebogenaktionen die Antwortdaten online übermitteln möchten, bietet sich das „Einmal-Kennwort-Verfahren“ an. Die versicherte Person erhält auf dem Postweg ein Einmalpasswort, über das nur ein festgelegter Vorgang aufgerufen werden kann. Dies ermöglicht einen alternativen Zugang, ohne dass ein o.a. „Benutzer-Konto“ angelegt wird.

Das Einmal-Kennwort muss vom SV-Träger individuell für jede versicherte Person erzeugt werden. Es muss sichergestellt sein, dass das gleiche Kennwort nicht mehrfach für verschiedene Versicherte erzeugt wird. Die entsprechenden Vorgaben zur Generierung von Kennwörtern

[47] Die Nutzung einer mTAN ist zu bedenken, denn die Handynummer kann später für die Gerätebindung als weiterem Modul der Authentifizierung genutzt werden.

gem. dem IT-Grundschutzkompendium des BSI (Modul ORP.4) und dem Modul M 2.11 des bisherigen Grundschutzkatalogs[48] sind zu beachten.

Das Einmal-Kennwort ist den Versicherten postalisch zu übermitteln (Zwei-Faktor-Authentifizierungsverfahren), in welchem das Eingabeverfahren beschrieben werden sollte. Ferner ist über die festgelegte Gültigkeitsdauer des Kennwortes (max. 60 Tage) und dessen Verfall zu informieren, sobald die versicherte Person den damit verbundenen Online-Geschäftsprozess vollständig durchgeführt hat. Wird der mit dem Kennwort verknüpfte Eingabeprozess vorzeitig abgebrochen, sollte das Kennwort für eine Wiederaufnahme weiter genutzt werden können.
Die vergebenen Einmal-Kennwörter sind beim SV-Träger in einer geschützten Datenbank solange zu speichern, bis der dazugehörige Prozess abgearbeitet wurde oder die Verfallfrist abgelaufen ist. Es ist sicherzustellen, dass die Sachbearbeitung zu keinem Zeitpunkt Einblick in das Einmal-Kennwort hat.

Bei Übermittlung von Daten der Schutzklasse „substanziell / hoch“ können weitere (transaktionsbezogene / sitzungsbezogene) Sicherungsmittel erforderlich sein (siehe Punkt 4.2.3.2).

4.2.3.5 Authentifizierung bei Nutzung von Apps

Auch bei der elektronischen Kommunikation über Apps sind die allgemeinen Anforderungen zur Sicherung des Zugangs zur Kommunikation anzuwenden. Dies gilt insbesondere bei Übermittlung sensibler Daten.

Entsprechend der Schutzbedarfsfeststellung / Risikoanalyse sind die Anforderungen entsprechend dem Schutzbedarf der elektronischen Kommunikation auszugestalten:

- Für eine Authentifizierung bei einer Online-Geschäftsstelle über eine App gelten die Ausführungen zur Online-Kommunikation.
- Bei einer Kommunikation mit dem Application-Server hat bei der Erstanmeldung zum System mindestens eine Zwei-Faktor-Authentifizierung zu erfolgen. Dies kann auf folgendem Weg geschehen:
  - Erstidentifikation am Server
  - Mitteilung der Zugangsdaten über Post
  - Die Authentifizierung am Application-Server erfolgt über die per Post mitgeteilten Geheimnisse / Zugangsdaten.
- Das zur Authentisierung genutzte Schlüsselmaterial sollte in einer sicheren Umgebung gespeichert und angewandt werden.[49]
- Bei Übermittlung von Daten der Schutzklasse „substanziell / hoch“ sind weitere (sitzungsbezogene / transaktionsbezogene) Sicherungsmittel erforderlich.
- Eine Authentifizierung des mobilen Gerätes und der Ausschluss der Kommunikation mit an-

[48] Grundschutzkompendium Modul ORP.4 abrufbar unter:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html

Modul M 2.11 des bisherigen Grundschutzkatalogs abrufbar unter:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02011.html

[49] Die SV-Träger sollten vorab festlegen, was als sicher angesehen wird:
- Versionen der Handys
- Sandbox
- Konzept
- Updates,
- Weiterentwicklungsverfahren

deren Geräten als dem authentifizierten kann das Sicherheitsniveau steigern.
Ggf. sollten gerootete Geräte ausgeschlossen werden!
- Für einfache Datenabrufe ohne personenbezogene Daten über einen Application-Server empfehlen die Prüfdienste eine Nutzung der App ohne Anmeldung zu ermöglichen.

Die Mindestanforderungen für alle Fälle der App-Kommunikation sind:

- Die App darf keine nutzerbezogenen Daten ungesichert auf dem Gerät speichern. Diese Daten sind auf dem Application-Server gesichert vorzuhalten.
- Während der Nutzung der App gespeicherte Daten sind in einem gesicherten Bereich abzuspeichern.

4.2.4 Umsetzung der eIDAS-Verordnung

Die eIDAS-Verordnung[50] legt einen einheitlichen Rechtsrahmen für den elektronischen Identitätsnachweis und für Vertrauensdienste (z. B. elektronische Signaturen, Siegel und Zeitstempel) fest. Die Umsetzung der Verordnung in deutsches Recht erfolgt durch das Vertrauensdienstegesetz (VDG).[51] Die Instrumente der Verordnung sollten bei der Gestaltung der Authentifizierungs-/ Identifikationskonzepte der SV-Träger im Rahmen der elektronischen Kommunikation in die Überlegungen einbezogen werden.

Organisationszertifikate
Die Bedeutung der Organisationszertifikate, deren Anwendung im deutschen Recht durch § 17 VDG erfolgt, liegt in der Wirkung als Herkunftsnachweis. Das Zertifikat stellt keinen Ersatz der persönlichen Unterschrift dar, kann aber den Nachweis der Authentizität (auch bei Bescheiden) erbringen. Technisch entsprechen die Zertifikate einer elektronischen Signatur, sind aber „nur“ einer juristischen Person zugeordnet.
Dadurch wird ein organisationsweiter bzw. steuerbarer (nach Funktion, Bevollmächtigung, Berechtigung) Einsatz möglich, ohne dass – wie bei der elektronischen Signatur - Zertifikate für jeden Mitarbeiter der juristischen Person erforderlich sind.

Elektronische Einschreibe- und Zustelldienste
Elektronische Einschreiben (§ 18 VDG) betreffen die Übermittlung von Daten mit elektronischen Mitteln. Erreicht werden kann dadurch der Nachweis für die Absendung durch identifizierte Absender sowie Zustellung / Empfang der Daten / Nachricht bei identifizierten Empfängern zu einem nachvollziehbaren Zeitpunkt. Auch die Rechtswirkung der Unversehrtheit der Daten, also der Schutz vor Verlust oder unbefugter Änderung (Integrität), ist gegeben.

Fernsignaturen
Fernsignaturen, die im VDG nicht geregelt sind, so dass die Bestimmungen der eIDAS-Verordnung nach Ansicht der Prüfdienste herangezogen werden können, beinhalten die Möglichkeit der Verwendung einer QES ohne Smartcard / Lesegeräte.
Dadurch kann eine Authentifizierung auf hohem Niveau und gleichzeitig eine Nutzbarkeit für mobile Dienste erreicht werden.
Das Signaturverfahren verläuft dann – grob dargestellt – wie folgt:

- Grundlegende Authentifizierung des Anwenders für die Fernsignatur bei einem Vertrauens-

[50] Verordnung (EU) Nr. 910 / 2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

[51] Gesetz vom 18. Juli 2017, BGBl. 2017 I, S. 2745.

diensteanbieter (Identitätsfeststellung beim Vertrauensdiensteanbieter durch Zwei-Faktor-Authentifizierung)
- Speicherung der Signaturschlüssel in sicheren Einheiten
- Vertrauensdienstanbieter versendet Code zum Auslösen der Fernsignatur an mobiles Gerät des Anwenders
- Auslösen der Fernsignatur beim Vertrauensdiensteanbieter über Code am (mobilen oder anderen) Gerät
- Vertrauensdienstanbieter gibt nach Empfang des Codes des Anwenders das Signaturzertifikat für die Fernsignatur frei
- Als ggf. weitere (zweite) Faktoren können bei hohem Schutzbedarf dann weitere, auch auf mobilen Geräten einsetzbare Faktoren dienen (z. B. biometrische Funktionen)

4.3 Behandlung der Online-Daten und Daten mittels Apps

4.3.1 Datenumfang und Dokumentation

Zur Übermittlung der von Versicherten eingegebenen Daten ist vor Beginn der Eingabe eine verschlüsselte Verbindung zwischen dem Eingabegerät und dem Server des SV-Trägers aufzubauen. Für Daten mit einem normalen Schutzbedarf ist eine TLS-Verschlüsselung ausreichend.[52] Mindestens sind Schutzmaßnahmen zu ergreifen, die dem jeweils aktuellen Stand der Technik entsprechen, und deren kryptographische Verfahren eine angemessene Sicherheit bieten. Bei den im Rahmen der Schutzbedürftigkeit als „substanziell“ oder „hoch“ zu bewertenden Daten muss der SV-Träger entscheiden, ob hierbei zusätzliche Schutzmaßnahmen zu nutzen sind.

Der SV-Träger hat einen Nachweis darüber zu führen, dass die Daten durch die Versicherten übermittelt wurden (Authentifizierung, Nichtabstreitbarkeit), wann sie in seinen Zugangsbereich gelangt und dass sie dort nicht verändert worden sind (Integrität). Die empfangenen Daten lassen sich unterteilen in Nutzdaten und Metadaten:

Nutzdaten sind die von den Versicherten während des Online-Prozesses eingegebenen Angaben. Sie sind – zusammen mit der entsprechenden Frage / Bezeichnung des Eingabefeldes – zu speichern (Hinweis: Die Speicherung der „Frage“ ist als Kurzform / Schlagwort möglich).

Metadaten sind systemseitig erzeugte Zusatzdaten, anhand derer der SV-Träger belegen kann, dass die Nutzdaten durch die Versicherten erzeugt wurden. Hierzu gehören insbesondere

- eindeutiges Identifizierungsmerkmal der versicherten Person (ggf. auch Benutzername)
- Eingabeweg (Benutzer-Konto oder „Einmal-Kennwort-Verfahren“)
- Systemzeit der Übermittlung der Daten (Datum, Uhrzeit)

Sowohl die im Online-Prozess erhobenen Nutzdaten als auch die Metadaten sind in einer Datendatei zu speichern. Diese Datei muss bei späteren Prüfungen (z. B. RSA-Prüfung) maschinell ausgewertet werden können. Hierzu ist es erforderlich, dass die Speicherung in einem zukunftssicheren Datenformat erfolgt. Das BSI empfiehlt hierzu u.a. das XML- oder csv-Format. Aber auch eine Speicherung als Textdatei (mit fester Satzlänge) wäre für die Prüfdienste auswertbar. Der Satzaufbau ist einheitlich zu gestalten. Fragen, die der Versicherte nicht beantworten muss, sind trotzdem aufzuführen und das Ergebnisfeld mit „blank“ zu verse-

[52] Derzeitiger Stand der Technik ist die TLS-Verschlüsselung 1.2. Seit 2018 ist TLS 1.3 der offizielle Standard für Transportverschlüsselung.

hen.

Neben dieser Datendatei sollte der SV-Träger aus den generierten Antworten ein PDF-Dokument erstellen, welches sich der Versicherte anzeigen und herunterladen kann. Auch dieses sollte die Nutz- und die Metadaten enthalten.

4.3.2 Integritätsschutz

Die unter Punkt 4.3.1 aufgeführten Dateien (Daten und PDF-Datei) sind unmittelbar nach ihrer Erzeugung gegen einen möglichen Integritätsverlust zu schützen. Dies kann automatisiert durch folgende Verfahren erfolgen:

- Automatische Anbringung einer QES
- Automatische Anbringung eines elektronischen Siegels
- Automatische Anbringung eines qualifizierten elektronischen Zeitstempels eines qualifizierten Vertrauensdiensteanbieters
- Automatische Anbringung einer fortgeschrittenen Signatur gem. eIDAS-Verordnung
- Automatische Anbringung einer PGP-Signatur, die mit einem ausreichend sicheren Schlüssel erzeugt wurde

Der SV-Träger hat bei der Entscheidung über die Wahl des Integritätsschutzes die Grundsätze der Wirtschaftlichkeit zu beachten. Eine Kosten- / Nutzen-Analyse (Wirtschaftlichkeitsbetrachtung) ist der Aufsichtsbehörde bei der Anzeige des Verfahrens vorzulegen.

4.3.3 Revisionssichere Archivierung / Langzeitspeicherung

Die unter Punkt 4.3.1 aufgeführten Dateien (Daten und PDF-Datei) müssen unmittelbar nach Eingang beim SV-Träger / Dienstleister und vor dem Einspielen in eine Fachanwendung auf nicht wieder beschreibbaren Datenträgern oder in einem revisionssicheren Archiv gespeichert werden.

Die Datensätze müssen während der Aufbewahrungsfristen lesbar gemacht bzw. für eine Auswertung über Prüftools zur Verfügung gestellt werden können.

Der Zugriff auf die archivierten Daten ist in einem Benutzerkonzept festzulegen. Administrationsrechte mit der Möglichkeit der Veränderung / Löschung von Daten sind restriktiv zu vergeben.

Der Zugriff sowie die Veränderung / Löschung von Daten sind zu dokumentieren.

Es wird empfohlen, die in der TR-03125 (TR-ESOR) des BSI enthaltenen Anforderungen an eine beweiswerterhaltende Archivierung elektronischer Daten / Dokumente zu berücksichtigen (siehe Punkt 7.3).

4.3.4 Apps

Die unter den Punkten 4.3.1 bis 4.3.3 genannten Anforderungen gelten ebenso für mittels Apps an einen Server übermittelte Daten und auf diesem Kommunikationsweg beigefügte Dokumente.

Die Software und die Datenströme sind zu beschreiben und die damit in Verbindung stehenden Anforderungen an Datenschutz, Datensicherheit, Integritätsschutz, Dokumentation und Spei-

cherung in einer Verfahrensdokumentation festzuhalten. Die Erfüllung dieser Bedingungen ist für die Erstellung einer Datenschutzfolgenabschätzung unumgänglich.

Als Mindestanforderung an die Sicherung der Übermittlungswege ist die Absicherung der Kommunikationsverbindung App / Back-End durch eine geeignete Transportverschlüsselung vorzusehen.

Die Datenintegrität auf dem Transportweg und bei der Speicherung ist zu gewährleisten. Nach erfolgter Schutzbedarfsanalyse sollten bei substanziellem / hohem Schutzbedarf auch kryptographische Maßnahmen vorgesehen werden.

4.4 Elektronische Einreichung von Nachweisen

4.4.1 Einreichung durch die Versicherten

Nach § 5 Abs. 1 EGovG können vorzulegende Nachweise (Dokumente, Bescheinigungen, Urkunden etc.) auch elektronisch eingereicht werden. Dabei entscheidet der SV-Träger nach pflichtgemäßem Ermessen, welche Art der elektronischen Einreichung zur Ermittlung des Sachverhalts zulässig ist.

Von diesem Grundsatz gibt es zwei Ausnahmen:

- Eine (andere) Rechtsvorschrift bestimmt, dass die Nachweise im Original (Papierform) vorzulegen sind.
- Der SV-Träger verlangt – nach pflichtgemäßem Ermessen – für bestimmte Verfahren oder im Einzelfall die Vorlage eines Originals.

In der Verwaltungspraxis wird bereits heute häufig die Vorlage von (nicht beglaubigten) Kopien zugelassen. Nach dem Willen des Gesetzgebers soll dies zur Regel werden, wenn die Vorlage eines Originals nicht durch Rechtsvorschrift angeordnet ist oder der SV-Träger sie in Ausübung seines Verfahrensermessens (§ 21 SGB X) für bestimmte Verfahren oder im Einzelfall verlangt.

Die Anforderungen an die bildliche und textliche Übereinstimmung gem. § 110a Abs. 1 SGB IV sind auch an dieser Stelle entsprechend heran zu ziehen.

Für den Fall, dass Zweifel an der Echtheit der elektronischen Kopie bzw. der Übereinstimmung mit dem Original bestehen, sollte der SV-Träger die Vorlage im Original verlangen.

Die vom SV-Träger zu bestimmende Art der Einreichung umfasst auch die Frage, in welchem Format ein elektronisches Dokument einzureichen ist.

Die durch Versicherte übermittelten elektronischen Nachweise sind vom SV-Träger gegen Integritätsverlust zu schützen und revisionssicher zu archivieren.
Ein entsprechendes Risikomanagement (siehe auch Punkt 5.1.3) sollte eingerichtet werden, innerhalb dessen Dokumente nicht nur auf ihre Lesbarkeit geprüft werden, sondern stichprobenartig oder in Verdachtsfällen auf ihre Echtheit. Die Träger sollten ihre Versicherten darauf hinweisen, dass Originalbelege zu diesem Zweck für einen gewissen Zeitraum aufbewahrt werden sollten. Im Rahmen des Risikomanagements sollten die Träger für sich eine Stichprobengröße festlegen, die zu Beginn / nach Einführung eines Systems größer ausfallen und im Verlauf in Abhängigkeit von den Erkenntnissen angepasst werden kann.

Es ist zu beachten, dass für Versicherte weiterhin die Möglichkeit bestehen muss, ihre Unterlagen schriftlich einzureichen.

4.4.2 Elektronische Übermittlung von Nachweisen zwischen verschiedenen Behörden / SV-Trägern

In § 5 Abs. 2 EGovG ist geregelt, dass die zuständige Behörde bei der Durchführung eines elektronischen Verwaltungsverfahrens erforderliche Nachweise, die von einer deutschen öffentlichen Stelle stammen, mit Einwilligung des Verfahrensbeteiligten (die Versicherten) direkt bei der ausstellenden öffentlichen Stelle elektronisch einholen kann. Zusätzlich wird in Absatz 2 die Form der elektronischen Einwilligung festgelegt.

Für den Bereich der gesetzlichen Sozialversicherung ist der Schutz der Sozialdaten in den §§ 67 – 80 SGB X geregelt. Nach § 67a Abs. 2 SGB X sind Sozialdaten grundsätzlich beim Betroffenen (Versicherte / Mitglieder) zu erheben[53]. Ohne seine Mitwirkung dürfen die Daten nur unter den in § 67a Abs. 2 Nr. 1 und 2 SGB X und der DS-GVO genannten Voraussetzungen erhoben werden.

Da das SGB X im Verhältnis zum EGovG hinsichtlich der Erhebung von Daten gleich- oder entgegenstehende Regelungen enthält, haben diese Vorrang (§ 1 Abs. 4 EGovG). Für die Übermittlung elektronischer Nachweise zwischen SV-Trägern gelten somit die in § 5 Abs. 2 und 3 EGovG enthaltenen Bedingungen nicht. Für die Form der Einwilligung geht die in § 67b Abs. 2 SGB X enthaltene Regelung der im EGovG vor.

4.5 Elektronischer Posteingang

4.5.1 Behandlung eingehender Fax-Sendungen

Der SV-Träger hat die Einsatzbedingungen über die Fax-Nutzung in einer Sicherheitsleitlinie detailliert festzulegen.

Elektronische Faxe[54]

Auch die auf einem Fax-Server eingehenden Faxe müssen – sofern keine Header- Informationen des Absenders vorhanden / sichtbar sind – mit einem elektronischen Fax-Stempel versehen werden.

Diese Faxe können wie folgt archiviert werden:

a) In Papierform (Ausdruck des Fax, siehe Punkt 3.3.2 zur weiteren Speicherung) oder
b) als Image, sofern dieses nach Eingang (und ggf. Anbringung eines Fax-Stempels) und vor der ersten Zugriffsmöglichkeit durch einen Mitarbeiter automatisch mit der qualifizierten Signatur eines (System-)Verantwortlichen oder einem qualifizierten Zeitstempel (der eine QES beinhaltet) versehen wurde (es gelten die Ausführungen zu „E-Mails“ in Punkt 4.5.2).

Hinweis:
Das unter b) beschriebenen Verfahren dient ausschließlich dem Integritätsschutz des Dokumentes.

Interne Weiterleitung von elektronischen Faxen
Die interne Weiterleitung elektronischer Faxe bzw. das elektronische Weiterfaxen an eine ande-

[53] „Erheben“ ist das Beschaffen von Daten über den Betroffenen (§ 67 Abs. 5 SGB X).

[54] Zu Papier-Faxen siehe Punkt 3.3.2.

re Dienststelle ist unter folgenden Voraussetzungen unkritisch:

- Die Fax-Server befinden sich in einer gesicherten Umgebung. Zugriff hat ausschließlich der zuständige Administrator.
- Die Übermittlungswege zwischen Fax-Server und Clients sind gegen innere und äußere Eingriffsmöglichkeiten durch Unbefugte geschützt. Maßgeblich sind hier die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in den BSI-Grundschutzkatalogen festgelegten Empfehlungen zur Netzsicherheit.
- Die jeweils zuständigen Beschäftigten (Fax-Server-Admin, Sachbearbeiter) verfügen über keine Bildbearbeitungssoftware, mit der der Inhalt des Fax verändert werden könnte.

4.5.2 Annahme und Speicherung eingehender E-Mails

Grundsätzlich müssen elektronisch bei dem SV-Träger eingehende Nachrichten / Dokumente, die eine rechtliche Wirkung entfalten, im elektronischen Langzeitarchiv gespeichert werden (§ 110a SGB IV). Dies gilt auch für E-Mails.
Voraussetzung hierfür ist, dass der SV-Träger / Dienstleister detailliert die nachfolgend genannten technischen und organisatorischen Maßnahmen festlegt und umsetzt:

- Ausführliche Verfahrensbeschreibung (einschl. Festlegung des Datenformates, z. B. automatische Umwandlung des Text- in ein PDF/A-Format)
- Festlegung (im Rahmen einer Risikoanalyse), welche Dokumente per E-Mail angenommen und anerkannt werden können (insbesondere im Hinblick auf eine notwendige Authentifizierung)
- Absicherung des gesamten Geschäftsprozesses gegen unbefugte Eingriffsmöglichkeiten zwischen Eingang auf dem Server und Übergabe an die Sachbearbeitung bzw. das Archiv
- bei Einsatz einer Einzelsignatur (durch die Sachbearbeitung) vor der Archivierung ist ein Verfahren zu entwickeln, das eine Manipulationsmöglichkeit des Dokumentes verhindert
- Festlegung, was mit Dokumenten zu geschehen hat, die nicht in das Langzeitarchiv gehören (z. B. unzuständiger Empfänger, SPAM, Dokumente mit extremen oder sexistischen Inhalten)

Elektronische Dokumente, die der **Absender nicht qualifiziert signiert** hat, sind vor der Langzeitspeicherung mit der QES eines (System-)Beschäftigten zu versehen, der für die „Betreuung“ des E-Mail- / Fax-Servers verantwortlich ist. Die Signatur kann im Wege der Massensignatur erfolgen. Alternativ ist auch eine Einzelsignatur durch den Empfänger (Sachbearbeiter) möglich. Der Integritätsschutz kann auch über die in Punkt 4.3.2 aufgeführten alternativen Sicherungsmittel erreicht werden.

Hinweis:
Die an diesen Dokumenten angebrachte Signatur dient ausschließlich dem Integritätsschutz des Dokumentes.

4.5.2.1 Über Portale / Anwendungen eingehende E-Mail

Bei über Portale oder Anwendungen eingehenden Mitteilungen / Nachrichten sind technische Verfahren zur Authentifizierung und Übertragung der Daten vorzusehen. Der Absender muss sich jeweils am Portal bzw. der Anwendung authentifizieren („anmelden“), um eine Nachricht an den SV-Träger senden zu können. Diese Form des Übermittlungsweges bietet folgende Vorteile:

- Eindeutige Authentifizierung des Absenders
- Anerkennung übermittelter Informationen als Beleg (z. B. bei RSA-Prüfungen)
- Eingang der Daten über eine gesicherten Übermittlungsweg (Verschlüsselung)

- Differenzierte Vorgangssteuerung über Funktionspostfächer für die Sachbearbeitung
- Eingrenzungsmöglichkeit der Dokumentenformate und Dokumentengröße
- Minimierung des Risikos, SPAM und andere nicht erwünschte Daten annehmen zu müssen

Die Prüfdienste empfehlen den SV-Trägern **dringend**, ihr bisheriges E-Mail-Eingangskonzept zu überarbeiten und in diesem Sinne umzustellen!

4.5.2.2 E-Mail-Eingang ohne Authentifizierung des Absenders

Bei einer „normalen“ **E-Mail** (ohne QES) ist die Authentizität des Absenders nicht nachprüfbar. Somit kann aus dieser zunächst keine rechtliche Wirkung gezogen werden. Aufgrund der grundsätzlich bestehenden Formfreiheit kann sie jedoch für die Ingangsetzung eines Verwaltungsverfahrens herangezogen werden, in dessen Verlauf dann Angaben beweissicher erhoben werden müssen.
Enthält eine solche Mail einen Anhang, der die QES des Absenders beinhaltet, sind Mail und Anhang zu speichern.

4.5.3 Speicherung eingehender De-Mails im elektronischen Langzeitarchiv

Nachrichten mit Schriftformerfordernis:
De-Mail-Nachrichten, die mit der Versandart nach § 5 Abs. 5 DeMailG (absenderbestätigt) beim SV-Träger eingehen, sind mit einer QES des De-Mail-Dienstanbieters des Absenders versehen. Diese Nachrichten enthalten außerdem die Daten der „sicheren Anmeldung“ als Metadaten. Die Nachricht ist zusammen mit den Metadaten und der QES im elektronischen Langzeitarchiv des SV-Trägers zu speichern. Das Anbringen einer neuen „Eingangssignatur“ durch den SV-Träger ist nicht erforderlich.

Es wird ausdrücklich darauf hingewiesen, dass die durch den De-Mail-Dienstanbieter angebrachte QES ausschließlich dem Integritätsschutz des Dokumentes dient.

Nachrichten ohne Schriftformerfordernis:
Diese müssen gem. DeMailG keine Absenderbestätigung und somit auch keine QES enthalten. Der Absender muss zur Erstellung auch keine „sichere Anmeldung“ am De-Mail-Account wählen.
Um der geltenden Archivierungspflicht gem. § 110a SGB IV zu genügen, sollten die SV-Träger diese De-Mail-Nachrichten (einschließlich etwaiger Metadaten) mit einer serverbasierten Eingangssignatur (QES) oder einem in Punkt 4.3.2 aufgeführten alternativen Sicherungsmittel versehen und im Langzeitarchiv speichern.

Es wird ausdrücklich darauf hingewiesen, dass diese Sicherungsmittel ausschließlich dem Integritätsschutz des Dokumentes dienen.

4.6 Elektronischer Postausgang

4.6.1 Grundsätze

Für den Bereich der gesetzlichen Sozialversicherung gilt grundsätzlich das Prinzip der Formfreiheit. So kann der **Erlass eines Verwaltungsaktes (VA)** z. B. auch mündlich erfolgen (siehe § 33 Abs. 2 Satz 1 SGB X). Es müssen lediglich die in § 33 Abs. 3 Satz 1 und ggf. Abs. 5 SGB X genannten Anforderungen (Erkennbarkeit der erlassenden Behörde) gewahrt werden. Dementsprechend kann z. B. bei einer Postausgangssignatur auf die QES grundsätzlich verzichtet werden.

Etwas anderes gilt nur dann, wenn für den VA die Schriftform angeordnet ist. In diesem Fall sind die in § 33 Abs. 3 bis 5 SGB X genannten Voraussetzungen zu erfüllen.

4.6.2 E-Mails (ohne / mit Anhang)

Ausgehende E-Mails (einschl. Anhänge) sollten in einem revisionssicheren Speichersystem / Langzeitarchiv unveränderbar gespeichert werden. Zur Sicherung der Integrität der Dokumente sollte ein entsprechender elektronischer Integritätsschutz (Punkt 4.3.2) angebracht werden.
Bei ausgehenden E-Mails[55] hat der SV-Träger unbedingt darauf zu achten, dass diese Mail keine personenbezogenen Daten / Sozialdaten enthält.

4.6.3 De-Mails (ohne / mit Anhang)

De-Mails, die schriftformersetzende Inhalte haben, müssen vom SV-Träger über eine „sichere Anmeldung“ und die Versandart nach § 5 Abs. 5 DeMailG versendet werden. Diese De-Mails werden vom De-Mail-Diensteanbieter des SV-Trägers mit einer QES versehen.

Bei Verwaltungsakten muss gem. § 33 Abs. 3 Satz 3 SGB X die Bestätigung nach § 5 Abs. 5 DeMailG die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lassen.

Bei der vom De-Mail-Diensteanbieter automatisiert angebrachten QES handelt es sich nicht um eine Willenserklärung des Absenders, hat also keine die Schriftform / Unterschrift der Absendenden ersetzende Wirkung. Diese QES ist jedoch als Integritätsschutz für das Dokument ausreichend. Eine revisionssichere Speicherung mit einem zusätzlich angebrachten Integritätsschutz (Signatur) ist möglich.

Für De-Mails ohne schriftformersetzende Inhalte gilt die Regelung zu Punkt 4.5.2.

4.6.4 Erstellung und Versand von Serienbriefen

Im Rahmen von elektronischen Workflows ist es üblich, Serienbriefe unter Verwendung vorgefertigter Textbausteine, z. B. als Bescheide, zu versenden. Aufgrund der Regelungen in § 110a SGB IV ist zu empfehlen, bei der Langzeitspeicherung die „Durchschriften“ derartig erzeugter Briefe mit einer QES des Absenders (oder einem alternativen Integritätsschutz gem. Punkt 4.3.2) zu versehen. Nach § 110a Abs. 2 Satz 3 SGB IV ist bei der Langzeitspeicherung nicht erforderlich, dass die Wiedergabe auf dem dauerhaften Datenträger mit der erstellten Unterlage (Brief an Versicherte) bildlich übereinstimmt. Das bedeutet, dass die elektronische „Durchschrift“ z. B. unter Aufführung der verwendeten Textbausteinnummern sowie der Variablen erfolgen kann. Die inhaltliche Übereinstimmung mit dem ursprünglich versandten Brief muss jedoch nachvollziehbar sein.
Im Rahmen der zunehmenden Verwendung von E-Akten ist es auch möglich, die Einzeldokumente in der jeweiligen E-Akte abzulegen.

Auf die Ausführungen im Abschnitt 5 „Automatisierte Sachbearbeitung“ wird verwiesen.

[55] Unverschlüsselt oder nicht authentifiziert

4.7 Soziale Netzwerke

Bei der Verwendung von Messaging- bzw. Kurznachrichtendiensten sowie sozialen Netzwerken zur Kommunikation mit Versicherten sind die vom Bundesversicherungsamt mit Schreiben vom 18.08.2017 bekannt gegebenen Grundsätze zur Einhaltung des Datenschutzes und der Datensicherheit zu beachten.[56]

[56] Abrufbar unter: https://www.bundesversicherungsamt.de/fileadmin/redaktion/Datenschutz_Datensicherheit/2017-08-18_Rundschreiben_SozNetze_MessagingDienste.pdf

5 Automatisierte Sachbearbeitung

5.1 Einleitung

Die (teil)automatisierte Sachbearbeitung ist eine Form der automatisierten Datenverarbeitung, bei der die Verarbeitung von Sachverhalten (teilweise) ohne Unterstützung oder gleichzeitigen Zugriff durch eine natürliche Person sich selbst organisierend und anhand vorgegebener technischer wie fachlicher Parameter abläuft. Von einer sog. „Dunkelverarbeitung“ wird gesprochen, wenn der Prozess vom Eingang der Daten bis zur Entscheidung (Feststellungsverfahren, Zahlungsanweisung etc.) und ggf. Versendung der Entscheidung an andere Stellen gänzlich ohne Zugriff natürlicher Personen abläuft.

Da durch die Automatisierung von Arbeitsabläufen Prozesse effizienter, schneller und kostengünstiger durchgeführt werden können und sollen, wird teil- oder vollautomatisierte Sachbearbeitung bereits bei vielen SV-Trägern in unterschiedlichem Umfang und unterschiedlichen Geschäftsfeldern angewendet. Die automatisierte Datenverarbeitung unterliegt im Hinblick auf die Ordnungsmäßigkeit der durch die Verarbeitung abgewickelten Geschäftsvorfälle und Prozesse besonderen Anforderungen.

Rechtsvorgaben / Hilfen / Unterlagen

- § 31a und § 37 SGB X
- § 110a SGB IV mit Grundsätzen der Aufbewahrung des GKV-Spitzenverbandes
- SVRV / SRVwV
- Handreichung IT-Planungsrat[57]

5.1 Anforderungen

Ziel der Umsetzung der unten stehenden Anforderungen ist, dass die Verfahren fachlich und technisch rechtmäßig sowie wirtschaftlich ablaufen und die grundlegenden Informationen (Originaldaten und Ergebnisse) als Belege Anerkennung finden können. Hierzu dienen die im Folgenden angeführten Anforderungen, die bei Einrichtung und Betrieb von Anwendungen der automatisierten Sachbearbeitung einzubeziehen sind.

5.1.1 Materielles Fachrecht

Das auf die Sachverhalte anzuwendende Recht ist in vollem Umfang auch bei automatisierten Schritten der Bearbeitung zu beachten.

- **SVRV / SRVwV**
  Die Vorschriften der Rechnungslegung (insbesondere die Regelungen der SVRV und der SRVwV) sind auch bei automatisierter Sachbearbeitung zu beachten.
  Zu nennen sind insbesondere die Vorgaben zu Zahlungsanordnung und Zahlungsfreigabe, Bestätigung der Vollständigkeit sowie rechnerischen und sachlichen Richtigkeit der Prozesse, die in entsprechender Weise technisch umzusetzen bzw. abzubilden sind (siehe weitere Ausführungen dazu unter Punkt 6.4).
  Das Verfahren ist in der Kassenordnung zu beschreiben.

[57] Abrufbar unter: https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/eID/Handreichung_Vertrauensniveaus.pdf

- **§ 31a SGB X**
  Der vollständig automatisierte Erlass von Verwaltungsakten als eine Erscheinungsform / ein Anwendungsfall der vollautomatisierten Sachbearbeitung ist (nur) unter bestimmten Bedingungen möglich:

  - So darf im Verfahren der Entscheidung zum Verwaltungsakt keine Bearbeitung durch einen Amtsträger erforderlich werden.
  - Die Vorschriften des SGB X sind einzuhalten.

  Dies bedeutet, dass für das Greifen des § 31a SGB X eine Datengrundlage vorhanden sein muss, die bereits an sich einen entscheidungsrelevanten und -reifen Sachverhalt abbildet und keine Entscheidungsalternativen, Bewertungen, Ermessensspielräume etc. aufweist. Eine eindeutige, strikte Schematisierung der Entscheidungsfindung, die keine weitere Entscheidung einer natürlichen Person als Sachbearbeitung mehr benötigt, muss daher gegeben sein.

- **§ 37 Abs. 2a SGB X**
  Die (rein) elektronische Bekanntgabe von Verwaltungsakten ist an Anforderungen und Anwendungsvoraussetzungen gebunden:

  - Es muss eine Einwilligung der Versicherten zu einer elektronischen Bekanntgabe vorliegen.
  - Für die Übermittlungsverfahren sind geeignete Identifizierungsmittel zu nutzen. Dabei ist davon auszugehen, dass die Inhalte von Verwaltungsakten regelmäßig dem Vertrauensniveaus substanziell und hoch zuzuordnen sind.
    Die Handreichung des IT-Planungsrates sieht für die Dokumentenübermittlung über Web-Upload für das dort verwandte Vertrauensniveau hoch+ z. B. die Nutzung der eID-Funktion des Personalausweises vor. Entsprechend sind auch die Authentifizierungsmittel – ggf. innerhalb eines Modulsystems - zu wählen (siehe Punkt 4.2 „Authentifizierung“).
  - Neben der Authentifizierung bei Übermittlung sollten die entsprechenden Konzepte auch eine sichere Benachrichtigung über die Bereitstellung des Verwaltungsaktes vorsehen. Dabei sollten bereits hierbei sichere Identifikationslösungen vorgesehen werden.
  - Der elektronische Verwaltungsakt muss durch die Versicherten in ihren eigenen Bereichen speicherbar sein.
  - Die Protokollierung des Abrufs des Verwaltungsaktes durch die Versicherten sollte seitens der SV-Träger erfolgen und die entsprechenden Abrufdaten revisionssicher gespeichert werden (Nachweis des Zugangs).

5.1.2 Dokumentation zur automatisierten Sachbearbeitung

Die automatisierte Sachbearbeitung stellt besondere Anforderungen an die Dokumentation, insbesondere da einzelne Arbeitsschritte in konkreten Verfahren nur über die parametrisierten Programmierungen erklärbar sind.

- Die grundlegenden Einstellungen (Parameter) der automatisierten Sachbearbeitung und die einzelnen Schritte der Sachbearbeitung (automatisiert sowie manuell) im konkreten Sachverhalt / Fall müssen nachvollziehbar für einen Dritten außerhalb des Systems des SV-Trägers (sachverständige Dritte) erkennbar sein.
- Verarbeitungsvorgänge sind (automatisch) zu protokollieren. Diese Protokollierung umfasst die Verarbeitungsschritte und Verarbeitungsdaten selbst sowie die dazugehörigen sog. Metadaten (insbesondere: Wer hat wann welchen Prozess angestoßen bzw. welcher automatisierte Verarbeitungsschritt hat wann mit welchem Versionsstand gegriffen).

- Fehler und Verarbeitungsabbrüche sind zu dokumentieren. Der zuständige Fachbereich des SV-Trägers sollte die Fehler und Verarbeitungsabbrüche im Hinblick auf ggf. bestehenden Anpassungsbedarf auswerten.
  Die Dokumentation kann insbesondere im Rahmen des internen Qualitätsmanagements bzw. der Prüfungen des Internen Kontrollsystems (IKS) herangezogen werden.
- Es muss eine (revisionssichere) Archivierung der Verarbeitungsdokumentation erfolgen (Verarbeitungsdaten und Metadaten hierzu).

5.1.3 Kontroll- und Prüfungsumfeld / Risikomanagement

Die automatisierte Sachbearbeitung (Aufbau und Betrieb) erfordert einerseits deren Einbeziehung in das „normale“ Umfeld der Kassenverfahrens (siehe auch Abschnitt 1), andererseits aber auch spezielle, aus der Besonderheit der technischen Datenverfahren resultierende Anforderungen in fachlicher und organisatorischer Hinsicht.

- Fachliche Anforderungen
  Die fachlichen Anforderungen, die an das interne Prüf- und Kontrollumfeld einer „normalen“ Sachbearbeitung zu stellen sind, sind auch bei einer automatisierten Sachbearbeitung zu erfüllen. Dies gilt für das materielle Fachrecht ebenso wie für die Vorschriften der Rechnungslegung (siehe oben).

- Umsetzung der Anforderungen des Internes Kontrollsystems
  Die automatisierte Sachbearbeitung ist auf die Vorgaben des IKS einzustellen.
  Das Interne Kontrollmanagement seinerseits hat die Verfahren der automatisierten Sachbearbeitung in ihren allgemeinen wie speziellen Anforderungen in das Kontrollkonzept und Prüfgeschehen einzubeziehen.

- Risikomanagement
  Verfahren der Digitalisierung und Automation sind mit besonderen (Daten-)Risiken verbunden. Daher sind diese Verfahren vor Errichtung und bei Betrieb im Rahmen eines Risikomanagements besonders zu betrachten (siehe Abschnitt 1 „Risikomanagement“).
  Bei Verfahren der automatisierten Sachbearbeitung sind im Rahmen des Risikomanagements insbesondere Fragen zu Risiken bei der Verarbeitung von Daten (Datenverlust, Erreichbarkeit der Daten, Übermittlung von Daten an Stellen außerhalb des Systems des SV-Trägers) sowie die organisatorische Lauffähigkeit des Systems bzw. der konkreten Anwendung (Ausfallsicherheit, Arbeitsfähigkeit etc.) zu betrachten. Siehe hierzu auch die Ausführungen zu Punkt 4.4.1.

- Notfallmanagement
  Das Notfallmanagement (Business Continuity Management) ist aufzubauen bzw. bestehende Verfahren sind ggf. im Hinblick auf die neuen Verfahren der automatisierten Sachbearbeitung anzupassen.

- Verantwortlichkeit
  Für die einzelnen fachlichen Geschäftsprozesse, die mit Verfahren der automatisierten Sachbearbeitung unterstützt werden sollen, sind die fachlichen und technischen Verantwortlichen und deren Aufgaben bereits im Vorhinein festzulegen.
  Dies gilt auch für die Ausgestaltung der Verfahren der automatisierten Sachbearbeitung selbst. So ist die Verantwortung für die Festlegung der einzelnen fachlichen Parameter nachvollziehbar zu dokumentieren.

- Festlegung der Zugangs- und Zugriffsberechtigungen
  Gerade bei einer automatisierten Sachbearbeitung sind die Zugangs- und Zugriffsberechtigungen sowie die Möglichkeiten zur Änderung fachlicher Parameter sorgfältig festzulegen

und einzurichten (Rechte- / Rollen- / Nutzerinnenkonzept). Bei diesen Verfahren besteht aufgrund der möglichen Vielzahl der mit den Anwendungen automatisiert bearbeiteten Sachverhalte ein erhöhtes Risikopotential.

Das Konzept und seine Ausführung (Rechtevergaben, Nutzung der Rechte) sind im Verlauf – als Teil des IKS - zu kontrollieren. Diese Kontrollansätze sollten bereits bei Einrichtung der Anwendung / des Systems aufgebaut werden.

- „Manuelle“ Stichprobenprüfung
  Eine automatisierte Sachbearbeitung kann sich auf eine Vielzahl von Fällen / Sachverhalten auswirken. Dabei müssen im Vorhinein der fachliche Prozess und die auf ihn bezogenen fachlichen und technischen Parameter festgelegt werden. Daher können fehlerhafte bzw. nicht sinnvolle Parametersetzungen große Auswirkungen haben.

  Insbesondere mit Blickrichtung auf die Erfüllung der fachlichen Anforderungen sind daher regelmäßige Stichprobenprüfungen auf die Einhaltung der fachrechtlichen Vorgaben vorzusehen. Die Höhe der Stichproben sollte risikoorientiert festgelegt werden. Parameter hierfür können die Auswirkung des automatisierten Verfahrensschrittes / Verfahrens (Zahlung, Höhe der Zahlung, Bedeutung für die Versicherten etc.) und die Zahl der verarbeiteten Einzelprozesse sein.

  Diese Regeln sind auch im Risikomanagement und IKS zu verankern.

5.1.4 Change Management

Die Änderungen der Geschäftsprozesse der automatisierten Sachbearbeitung bergen fachlich z. T. die gleichen Risiken (Festlegung der richtigen fachlichen Parameter) sowie im organisatorisch-technischen Bereich verschiedene Risiken wie bei deren Aufbau.[58] Daher sollten die Geschäftsprozesse zur Änderung fachlicher und technischer Parameter der Sachbearbeitung allgemein festgelegt werden. In die Änderungsverfahren sollten auch jeweils die relevanten Stellen / Fachbereiche des SV-Trägers nach einem festen Geschäftsprozess verpflichtend eingebunden werden:

- Fachbereich (materielles Recht und Fachprozesse)
- IT-Bereich
- Datenschutz
- IT-Sicherheit
- Risikomanagement und Internes Kontrollsystem
- Speicherung und Archivierung

Eine nachvollziehbare Dokumentation auch des Änderungsprozesses ist dringend zu empfehlen, damit ggf. im Nachhinein noch mögliche Fehlerquellen bzw. Verbesserungsmöglichkeiten identifizierbar sind.

5.1.5 Datenintegrität, Datensicherheit und Datenschutz

Die Integrität der in die automatisierte Sachbearbeitung eingehenden

[58] Siehe Ausführungen im Abschnitt 1

(Original-)Daten ist zu wahren, insbesondere wenn diese als Beleg dienen sollen.
Auch die im Rahmen der Sachbearbeitung bearbeiteten Daten sind integer zu halten. Es muss dauerhaft nachvollziehbar sein, welche Änderungen der Daten durch technische wie manuelle Bearbeitungsschritte erfolgt sind.

Die Anforderungen der Datensicherheit und des Datenschutzes sind auch bei den einzelnen Verfahren der Sachbearbeitung zu erfüllen (siehe Abschnitt 1).
Die Risiken können bei Verfahren der automatisierten Sachbearbeitung höher sein, da ggf. bei Fehlern eine Vielzahl von Fällen betroffen sein kann. Daher sind diese Anforderungen sorgfältig zu betrachten.

Die revisionssichere Beständigkeit der Daten (Fachdaten, Metadaten) der automatisierten Sachbearbeitung auch bei Migration (kassenintern, Nutzung von Dienstleistungsunternehmen) ist bereits beim Aufbau von Anwendungen und spätestens vor konkreten Migrationsschritten zu beachten.
Die Anforderungen beziehen sich dabei auf alle denkbaren Schritte von Datenmigrationen, z. B.:

- bei Auslagerung der Daten in Archivsysteme
- bei Migration der Daten beim Austausch von Systemen / Anwendungen der automatisierten Sachbearbeitung
- bei Änderung von Inhouse-Formaten und Konvertierungsvorgaben.

5.1.6 Langzeitspeicherung

Nach Punkt 2.6 der Grundsätze ordnungsgemäßer Aufbewahrung gem. § 110a SGB IV[59] müssen - sofern Software zur automatisierten Sachbearbeitung eingesetzt wird - die durch die Software durchgeführten Änderungen am Datenbestand und die diesen Prozess anstoßenden Regeln und Personen nachvollziehbar dokumentiert werden. Dies gilt ebenso für das allgemeine Regelwerk dieser Software sowie für dessen Änderungen.

Aus Sicht von Prüfungen und Revision (auch der SV-Träger) ist neben der nachvollziehbaren Dokumentation der eingeführten / geänderten Regeln und Änderungen am Datenbestand ebenso wichtig, dass diese Dokumentation revisionssicher geführt wird. Damit kann dann auch unveränderbar der jeweilige Prozess nachvollzogen werden.

Auch die sog. Meta-Informationen (Regeln, ändernden Personen und die Informationen zu Änderungen des Datenbestandes) sind an sich Daten, die wiederum Aufbewahrungsfristen unterliegen können. Die Meta-Information und deren Aufbewahrungsfrist sind dabei abhängig von den Grunddaten, auf die sie sich beziehen.

Die Anforderungen an die Speicherung gelten auch für „Massenbriefe“ bzw. Serienbriefe, bei denen vorab festgelegte Inhalte an einen definierten Personenkreis versandt werden.
Systemseitig ist revisionssicher festzuhalten, welche Schreiben mit welchen Parametern (Adressatenkreis, Inhalt, in Bezug genommene Variablen, welcher Datenstand) versandt wurden.
Die Verknüpfung der inhaltlichen Daten zum Personenkreis / Adressatenkreis ist ebenfalls festzuhalten.

[59] Grundsätze ordnungsmäßiger Aufbewahrung im Sinne des § 110a SGB IV, Voraussetzungen der Rückgabe und Vernichtung von Unterlagen sowie Aufbewahrungsfristen für Unterlagen für den Bereich der gesetzlichen Kranken- und Pflegeversicherung, Version 3.0.

Das dem Versicherten zugesandte Dokument muss nicht als Einzel-Datei gesondert erstellt und revisionssicher gespeichert werden. Zu empfehlen ist jedoch, dass die Sachbearbeitung im System des SV-Trägers nachvollziehen kann, welche Informationen (Personenkreis, Inhalt, Datum) den Versicherten übermittelt worden sind.

Bei sog. eAkte-Anwendungen muss der Inhalt nachvollziehbar sein.[60] Die Bearbeitungsinformationen („Meta-Informationen“) und Inhalte müssen revisionssicher gespeichert werden.
Die Inhalte der eAkte-Anwendung müssen auslesbar und herstellbar sein.

Die gesetzlich vorgesehenen Aufbewahrungsfristen sind auch bei automatisierter Sachbearbeitung zu beachten. Hierzu können die Grundsätze der Aufbewahrung des GKV-Spitzenverbandes nach § 110a SGB IV (sog. Aufbewahrungskatalog) herangezogen werden.

Die Aufbewahrungsfristen beziehen sich auf folgende Daten

- die fachlichen Daten
- die Daten der Verarbeitungsdokumentation (sog. Metadaten)

Die entsprechenden Daten sind in geeigneten Archivsystemen aufzubewahren (siehe Abschnitt 7 „Langzeitspeicherung und Löschung“).

[60] Organisationskonzept elektronische Verwaltungsarbeit: https://www.verwaltung-innovativ.de/DE/E_Government/orgkonzept_everwaltung/orgkonzept_everwaltung_node.html

6 Elektronischer Datenaustausch

Der Austausch von Daten zwischen SV-Trägern und deren Partnern erfolgt in zunehmendem Umfang auf elektronischem Wege. Die Richtlinien der Spitzenverbände der Krankenkassen zum Datenaustausch sind grundsätzlich geeignet, einen sicheren Datentransfer zu gewährleisten. Danach ist die Identität des Absenders und die Authentizität der Daten sichergestellt.

Die in den Datensätzen enthaltenen Informationen werden häufig in verschiedene Datenbanken übernommen. Der Originaldatensatz als adäquates Gegenstück zum papiergebundenen Dokument (z. B. Originalrechnung) wird in der Regel nicht gespeichert bzw. nicht dauerhaft und unveränderbar gespeichert. Insbesondere erfordern es die RSA-Prüfungen, dass die Krankenkassen den Informationsstand zum Zeitpunkt der Abgabe der amtlichen Meldungen nachweisen können.

Bei einem papiergebundenen Dokument kann der Inhalt und der Zeitpunkt des Eingangs zweifelsfrei ermittelt werden. Bei einem Datensatz ist dies in der Regel nicht sichergestellt. Theoretisch könnte er noch unmittelbar vor der Einsichtnahme angepasst worden sein. Damit geht die Beweiskraft der Information verloren.

Um den Nachweis der Datenintegrität erbringen zu können, sind die im § 110a Abs. 1 SGB IV gestellten Anforderungen zu beachten. Danach sind Unterlagen, die für die öffentlich-rechtliche Verwaltungstätigkeit, insbesondere für die Durchführung eines Verwaltungsverfahrens oder für die Feststellung einer Leistung, erforderlich sind, nach den Grundsätzen ordnungsmäßiger Aufbewahrung[61] sicher zu speichern. Zu den „Unterlagen“ in diesem Sinne gehören auch Daten, die nur mit Hilfe einer Datenverarbeitungsanlage erstellt worden sind.

Daraus folgt, dass die SV-Träger bei der Annahme elektronischer Datensätze den Originaldatensatz im Sinne der Aufbewahrungspflichten nach § 110a SGB IV dauerhaft und unveränderbar zu speichern haben. Hierzu sind geeignete Archivsysteme zu nutzen, die eine Versionsintegrität gewährleisten (siehe hierzu Ausführungen zu nicht wieder beschreibbaren Datenträger unter Punkt 3.2.3). Der SV-Träger muss im Zweifelsfall den Nachweis erbringen, dass die Ursprungsdatensätze im Original vorliegen und nicht verändert wurden.

Die Daten müssen für Revisionszwecke zeitnah zur Verfügung stehen.

Die Auftragsdaten (Vorlaufdatensatz) und die Nutzdaten sind nach Eingang beim SV-Träger (oder beauftragten Dritten) direkt nach der Entschlüsselung elektronisch zu speichern. Zur Einsichtnahme der Daten ist die Möglichkeit zu schaffen, das Speicherformat (z. B. EDIFACT, XML, JSON) in eine lesbare Form umzuwandeln.

Werden die Daten nach der Speicherung des Original-Datensatzes in den operativen DV-Systemen verarbeitet, sind die vorgenommenen Datenänderungen in den Fachverfahren im Sinne einer Historienführung nachvollziehbar zu protokollieren.

6.1 Ergänzende rechtliche Grundlagen

§ 78 SGB IV bildet die Rechtsgrundlage, Grundsätze u. a. für die Zahlung, die Buchführung und die Rechnungslegung festzulegen. Die Regelung ist nach den Grundsätzen des für den Bund

[61] § 110c SGB IV bzw. Heranziehung der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD).

und die Länder geltenden Haushaltsrechts vorzunehmen. Diese hat die Besonderheiten der SV-Träger und der einzelnen Versicherungszweige zu berücksichtigen.
Aufgrund der Regelungskompetenz nach § 78 SGB IV wurden die Grundsätze des Rechnungswesens in der SVRV und Detailregelungen in der SRVwV festgelegt. Ergänzend hat der GKV-Spitzenverband in Zusammenarbeit mit der Informationstechnischen Servicestelle der gesetzlichen Krankenversicherungen GmbH (ITSG) insbesondere „Gemeinsame Grundsätze Technik für die elektronische Datenübermittlung gem. § 95 SGB IV“ erarbeitet.

Die Informationen können über die Internetseiten des GKV-Spitzenverbandes heruntergeladen werden (www.gkv-datenaustausch.de). Die Dokumente regeln detailliert die technischen Vorgaben der Datenfernübertragung und dem Datenträgeraustausch zwischen Arbeitgebern bzw. Leistungserbringern und SV-Trägern. Sie sind für die Beteiligten verbindlich.

6.2 Speicherung des Originaldatensatzes

Bei elektronischen Eingängen sind entsprechende Vorschriften zur Aufbewahrung der Daten zu erfüllen. In der Sozialversicherung sind dies Art. 5 und Art. 32 DS-GVO, § 67b Abs. 1 Satz 4 SGB X i.V.m. § 22 Abs. 2 BDSG, die SVHV sowie die SVRV i. V. m. der SRVwV.

§ 6 Abs. 3 SVRV stellt klar, dass Belege auch elektronisch erzeugte Dateien oder Datensätze sein können. Somit ist sichergestellt, dass die rechtlichen Anforderungen für Belege auch für elektronische Datensätze gelten.

Ergänzend fordern § 9 Abs.1 und 3 SRVwV, dass

- die Belege zu nummerieren und geordnet und sicher aufzubewahren sind. Bei elektronisch erzeugten Dateien oder **Datensätzen** muss insbesondere sichergestellt sein, dass die Daten **verfügbar** sind und innerhalb angemessener Frist **lesbar gemacht** und **ausgedruckt** werden können. Mehrausfertigungen von Belegen müssen als solche erkennbar sein und
- Berichtigungsbuchungen sind auf dem ursprünglichen Beleg zu vermerken und durch einen neuen Beleg zu begründen; sie brauchen auf dem ursprünglichen Beleg nicht vermerkt zu werden, wenn in der Kassenordnung ein gleichwertiges Verfahren vorgesehen ist.

In § 12 Abs. 2 SRVwV ist geregelt, dass Änderungen in den zahlungsbegründenden Unterlagen so auszuführen sind, dass die ursprünglichen Angaben lesbar bleiben; die Berichtigungen sind durch Beifügung des Namenszeichens des Ändernden und des Datums der Änderung zu bescheinigen.

Eine Speicherung des verschlüsselten Original-Datensatzes birgt die Gefahr, dass der ursprüngliche Verschlüsselungsalgorithmus zu einem späteren Prüfzeitpunkt nicht mehr zur Verfügung steht und somit ein Entschlüsseln nicht mehr möglich wird.
Es wird daher empfohlen, die Nutzdaten nach Eingang beim SV-Träger direkt nach der Entschlüsselung elektronisch zu speichern. Es muss eine Absicherung des gesamten Geschäftsprozesses gegen unbefugte Eingriffsmöglichkeiten zwischen Eingang auf dem Server und Übergabe an die Sachbearbeitung bzw. das Archiv gegeben sein.

Zur Einsichtnahme der Daten ist die Möglichkeit zu schaffen, das Speicherformat (EDIFACT; XML, JSON) in eine lesbare Form umzuwandeln.

6.3 Nachvollziehbarkeit der Datenspeicherung und -änderung (Historienführung)

Automatisierte Verfahren sind durch besondere technische und organisatorische Maßnahmen vor unbemerkter und unberechtigter Veränderung zu schützen. Die zur Sicherheit dieser Verfahren zu erlassene Dienstanweisung muss die in Art. 5 und Art. 32 DSVGO, § 67b Abs. 1 Satz 4 SGB X i.V.m. § 22 Abs. 2 BDSG erforderlichen technisch-organisatorischen Maßnahmen regeln. Insbesondere ist darauf hinzuweisen, dass Einzelheiten von Verfahrensänderungen und neu eingeführter Verfahren entsprechend der Anlage 9 zu § 40 SRVwV zu dokumentieren sind. Mit dieser Regelung wird der Einsatz moderner IT-Technik im Rechnungswesen berücksichtigt und die Prüfbarkeit von Abrechnungsverfahren (Verfahrens- und Systemprüfungen) sichergestellt. Aus der Dokumentation muss sich ergeben, dass das Verfahren entsprechend seiner Beschreibung durchgeführt worden ist.

Das gesamte Verfahren ist in einer ausführlichen Verfahrensbeschreibung darzustellen. Die Beschreibung der programmtechnischen Lösung hat zu zeigen, wo und wie die sachlogischen Forderungen in Programmen umgesetzt sind. Tabellen, über die die Funktionen der Programme beeinflusst werden können, sind wie Programme zu behandeln. Änderungen von Tabellen mit Programmfunktion sind in der Weise zu dokumentieren, dass für die Dauer der Aufbewahrungsfrist der jeweilige Inhalt einer Tabelle festgestellt werden kann.

Somit sind automatisierte Verfahren durch Regelungen von technischen und organisatorischen Maßnahmen vor unbemerkten und unberechtigten Veränderungen zu schützen. Die Anwendungen haben sicherzustellen, dass dokumentiert wird, wer zu welcher Zeit Änderungen an den Daten vorgenommen hat. Verfahrensänderungen sind so zu dokumentieren, dass die Prüfbarkeit des Abrechnungsverfahrens für einen sachverständigen Dritten darstellbar und nachvollziehbar sichergestellt ist.

6.4 Dokumentation und Prüfbarkeit der Buchführung

Nach den Vorschriften der SVRV sind die Grundsätze ordnungsmäßiger Buchführung zu beachten, Buchungen und Aufzeichnungen sind vollständig, richtig, zeitgerecht, geordnet und nachprüfbar für einen sachverständigen Dritten vorzunehmen. Änderungen in zahlungsbegründenden Unterlagen sind so auszuführen, dass die ursprünglichen Angaben lesbar bleiben; die Berichtigungen sind durch Beifügung des Namenszeichens des Ändernden und des Datums der Änderung zu bescheinigen. Alle Buchungen müssen belegt sein, und Belege können auch elektronisch erzeugte Dateien oder Datensätze sein.

Bei der Nutzung von IT-Verfahren sind die Sicherheitsanforderungen in einer Dienstanweisung (siehe § 40 SRVwV) zu bestimmen und zu dokumentieren. Auch bei fremderworbener Software, bei der Teile der Verfahrensdokumentation vom Software-Ersteller angefertigt werden, ist der Buchführungspflichtige für die Vollständigkeit und den Informationsgehalt der Verfahrensdokumentation verantwortlich.

Die Verfahrensdokumentation der Software muss insbesondere beinhalten:

- Beschreibung der sachlogischen Lösung
- Beschreibung der programmtechnischen Lösung
- Beschreibung, wie die Programmidentität gewahrt wird
- Datenintegrität
- Arbeitsanweisungen für den Anwender
- Rollen- und Berechtigungskonzept zu den relevante Zahlungsfunktionen
- Risikoanalyse
- Ordnungsmäßigkeitskonzept

Beschreibung der sachlogischen Lösung: Die sachlogische Beschreibung enthält die Darstellung der fachlichen Aufgabe aus der Sicht des Anwenders.
Diese soll folgende Punkte enthalten:

- Generelle Aufgabenerstellung
- Beschreibung der Anwenderoberflächen für Ein- und Ausgabe einschließlich der manuellen Arbeiten
- Beschreibung der Datenbestände
- Beschreibung von Verarbeitungsregeln
- Beschreibung des Datenaustausches
- Beschreibung der maschinellen und manuellen Kontrollen
- Beschreibung der Fehlermeldungen und der sich aus Fehlern ergebenden Maßnahmen
- Schlüsselverzeichnisse
- Schnittstellen zu anderen Systemen

Beschreibung der programmtechnischen Lösung: Die Beschreibung der programmtechnischen Lösung hat zu zeigen, wo und wie die sachlogischen Forderungen in Programm umgesetzt werden.

Beschreibung, wie die Programmidentität gewahrt wird: In der Beschreibung, wie die Programmidentität gewahrt wird, hat der Buchführungspflichtige nachzuweisen, dass die sachlogischen Forderungen durch die eingesetzten Programme erbracht werden bzw. erbracht worden sind. Hierzu gehören die präzise Beschreibung des Freigabeverfahrens mit Regelungen über Freigabekompetenzen, der durchzuführenden Testläufe und die dabei zu verwendenden Daten sowie Anweisungen für Programmkontrollen.

Datenintegrität: (siehe dazu Punkt 5.1.2)

Arbeitsanweisungen für die Anwender: Die Arbeitsanweisungen, die für den Anwender zur sachgerechten Erledigung und Durchführung seiner Aufgaben vorhanden sein müssen, gehören ebenfalls zur Verfahrensdokumentationen und sind schriftlich zu fixieren. Das ist insbesondere die Beschreibung der im Verfahren vorgesehenen manuellen Kontrollen und Abstimmungen. Die Schnittstellen zu vor- und nachgelagerten Systemen sind hierfür zu berücksichtigen.

Rollen- und Berechtigungskonzept für die Zahlungsfunktionen: Zur Abbildung des Vier-Augen-Prinzips und zur Bestätigung der sachlichen und rechnerischen Richtigkeit können Funktionen der eingesetzten Anwendungssysteme verwendet werden, soweit es hierfür ein differenziertes Rollen- und Berechtigungskonzept gibt. Hierdurch wird die Abbildung der verschiedenen Rollen, z. B. durch Abgleich der zugelassenen Personen mit den entsprechenden Berechtigungsstufen, ermöglicht. Um die elektronische Bestätigung revisionssicher zu machen, sind die jeweiligen Prüf- und Verarbeitungsschritte entsprechend zu protokollieren.

Gefährdungsanalyse: In einer Gefährdungsanalyse sind die Risiken zu ermitteln und zu bewerten (siehe dazu Punkt 5.1.3). Dabei sind die durch Fehler und Missbrauch bedingten haushaltswirtschaftlichen Auswirkungen gegen die zusätzlichen Ausgaben zur Erhöhung der Verfahrenssicherheit abzuwägen.
Bei der Bewertung sind höhere Risiken dann anzunehmen, wenn

- Geschäftsvorfälle zu wiederkehrenden Zahlungen führen und im voraussichtlichen Anspruchszeitraum den Betrag von 7.500 Euro übersteigen,
- Geschäftsvorfälle zu Zahlungen auf unbestimmte Zeit führen,
- Einmalzahlungen den Betrag von 2.500 Euro übersteigen,
- auf Forderungen verzichtet wird (z. B. Niederschlagung, Erlass),
- Verwahrgelder ausgezahlt werden oder
- Beträge als Vorschüsse gezahlt werden.

Ordnungsmäßigkeitskonzept: Im Ordnungsmäßigkeitskonzept sind die Einzelheiten zur Abgrenzung der Verantwortlichkeiten (Berechtigungskonzept) und die nachfolgenden Maßnahmen darzustellen. Es ist zu bestimmen, ob und inwieweit

- zwei oder mehr Personen maßgeblich an einem einzelnen Geschäftsvorfall zu beteiligen sind,
- nur eine Person den Geschäftsvorfall bearbeitet,
- eine Anordnung zusätzlich von einer weiteren Person zu prüfen und freizugeben ist,
- vollautomatisierte Verfahrensabläufe ohne Beteiligung einer Person Anwendung finden,
- zusätzliche Prüfverfahren einzusetzen sind und
- Sicherungsmaßnahmen zu treffen sind.

6.5 Neufassung Datenschutzrecht

Mit der Neufassung der datenschutzrechtlichen Vorschriften im SGB X sind auch Änderungen der Vorschriften über die Übermittlung von Daten verbunden (§§ 67d bis 80 SGB X).
Diese Änderungen sind bei der Gestaltung der Verfahren und Systeme der SV-Träger zu beachten.

6.6 Interoperabilität

Das von der Gesellschaft für Telematik (gematik) gem. § 291e Abs. 1 SGB V aufzubauende sog. Interoperabilitätsverzeichnis soll die Interoperabilität zwischen informationstechnischen Systemen im Gesundheitswesen fördern. Dabei soll im Sinne einer sinnvollen Nutzung ein übergeordneter Zweck des Datenaustausches impliziert sein.[62]
Die Anforderung eines möglichen Datenaustausches bzw. dessen technische Ermöglichung ist bei der Gestaltung der Systeme der Träger des Gesundheitswesens zu beachten.

6.7 Meldeverfahren EESSI

Die Anforderungen bzw. Schnittstellen für eine Anbindung des Systems des SV-Trägers im Hinblick auf den „Elektronischen Austausch von Sozialversicherungsdaten“ (EESSI) sind im Bereich des Datenaustausches zu beachten.

6.8 E-Mail-Datenaustauschverfahren

Im Rahmen von Datenaustauschverfahren zwischen SV-Trägern / Institutionen sind die Ausführungen zu Punkt 4.4.2 zu beachten.

6.9 Verfahren nach § 79 SGB X n.F.

Die technischen und verfahrensmäßigen Anforderungen an die automatisierten Verfahren zum Datenabruf (insbesondere nach Abs. 2) sind bei der Gestaltung dieser Verfahren zu berücksichtigen.

[62] Siehe Unterrichtung durch die Bundesregierung vom 12. Januar 2018, BT-Drs. 19 / 451, S. 2.

7 Langzeitspeicherung und Löschung elektronisch erzeugter Dokumente und Daten

7.1 Langzeitspeicherung

Grundsätzlich sind alle elektronisch vom SV-Träger erzeugten bzw. von Versicherten oder Dritten übersandten elektronische Dokumente, die für den jeweiligen Bearbeitungsvorgang bzw. das „Versicherungsleben“ der Versicherten rechtserheblichen Charakter („Beweischarakter“) haben, in einem elektronischen Langzeitarchiv aufzubewahren.
Hierzu gehören

Eingehende Dokumente:

- Elektronisch erzeugte Dokumente (z. B. im DOC- oder PDF-Format), die elektronisch an den SV-Träger gesandt wurden (z. B. auf Datenträger, E-Mail-Anhang, ftp)
- Eingegangene elektronische Faxe (z. B. auf Fax-Server)
- Eingegangene E-Mails, De-Mails und deren Anhänge
- Im Web-Formular auf der Internetseite des SV-Trägers erzeugte Daten im Text- oder PDF-Format

Ausgehende / erzeugte Dokumente:

- „Durchschriften“ der vom SV-Träger oder seinen Beschäftigten erzeugten elektronischen Dokumente, die elektronisch (und / oder in Papierform) an Externe versandt wurden (auch elektronische Faxe)
- Vom SV-Träger oder seinen Beschäftigten an Externe (z. B. Versicherte, Arbeitgeber, Leistungserbringer) versandte E-Mails, De-Mails und deren Anhänge
- Interne Vermerke, Verfügungen, Notizen, Protokolle

Die Anforderungen an die rechtssichere Langzeitspeicherung für diese Dokumente sind definiert durch die §§ 110a bis 110c SGB IV i. V. m. den Grundsätzen ordnungsgemäßer Aufbewahrung sowie dem EGovG.

Darüber hinaus ist die Sicherheit in der Verarbeitung gem. Art. 32 DSVGO zu beachten. Die technischen und organisatorischen Vorgaben ergeben sich aus § 67b Abs. 1 Satz 4 SGB X i. V. m. § 22 Abs. 2 BDSG.

Weiterhin sind die vom Verband Organisations- und Informationssysteme e. V. (VOI) aufgestellten Merksätze zur revisionssicheren elektronischen Archivierung zu beachten:

- Jedes Dokument muss unveränderbar aufbewahrt werden.
- Es darf kein Dokument auf dem Weg ins Archiv oder im Archiv selbst verloren gehen.
- Jedes Dokument muss mit geeigneten Retrievaltechniken wieder auffindbar sein.
- Es muss genau das Dokument wiedergefunden werden, das gesucht worden ist.
- Kein Dokument darf während seiner vorgesehenen Lebenszeit zerstört werden können.
- Jedes Dokument muss in genau der gleichen Form, wie es erfasst wurde, wieder angezeigt und gedruckt werden können.
- Jedes Dokument muss zeitnah wiedergefunden werden können.
- Alle Aktionen im Archiv, die Veränderungen in der Organisation und Struktur bewirken, sind derart zu protokollieren, dass die Wiederherstellung des ursprünglichen Zustandes möglich ist.
- Elektronische Archive sind so auszulegen, dass eine Migration auf neue Plattformen, Medien, Softwareversionen und Komponenten ohne Informationsverlust möglich ist.

- Das System muss dem Anwender die Möglichkeit bieten, die gesetzlichen Bestimmungen sowie die betrieblichen Bestimmungen des Anwenders hinsichtlich Datensicherheit und Datenschutz über die Lebensdauer des Archivs sicherzustellen.

7.2 Besonderheiten

7.2.1 Aufbewahrung von Fehler- / Bearbeitungslisten

Fehler- / Bearbeitungs- / Kontrolllisten möchten viele SV-Träger nicht mehr in Papierform ablegen, sondern in elektronischer Form speichern. Sofern diese Listen in den Grundsätzen ordnungsmäßiger Aufbewahrung aufgeführt sind, müssen sie aufbewahrt werden. Ansonsten ist eine Aufbewahrung in das Ermessen des SV-Trägers gestellt; er muss entscheiden, ob der Inhalt der Listen einen „rechtserheblichen Charakter“ besitzt.

In der Papierform sind die Listen einzuscannen und mit einer QES des Scan-Operators zu versehen (Nachvollziehbarkeit wer das Dokument wann in die elektronische Form überführt hat - § 67b SGB X i.V.m. § 22 Abs. 2 BDSG). In der elektronischen Form muss die (Druck-) Datei ebenfalls mit der QES / fortgeschrittenen Signatur des Bearbeiters bzw. einem elektronischen Siegel des SV-Trägers versehen im Langzeitarchiv gespeichert werden.

7.2.2 Aufbewahrungsfrist von Einzeldokumenten in eAkten / Vorgängen

Für die in einer elektronischen Akte (eAkte) aufzubewahrenden Einzeldokumente können gem. Aufbewahrungskatalog unterschiedliche Aufbewahrungsfristen gelten. In diesem Fall richtet sich der Endzeitpunkt der Aufbewahrungspflicht der Fallakte nach dem in ihr enthaltenen Einzeldokument mit der längsten Aufbewahrungsdauer. Diese „Verlängerung“ der Aufbewahrung verstößt nicht gegen das Löschgebot aus § 84 Abs. 2 Satz 2 SGB X, da die Fallakte einen Gesamtzusammenhang schafft, in dem eine Aufbewahrung zur allgemeinen Aufgabenerfüllung des SV-Trägers erforderlich sein kann.

7.3 Technische Richtlinie TR-03125 (TR-ESOR)

Das BSI hat mit der TR-03125 (TR-ESOR) ein Dokument zur Verfügung gestellt, das Orientierung und Hilfestellung gibt, um den vielfältigen Anforderungen hinsichtlich

- Verfügbarkeit und Lesbarkeit,
- Integrität und Authentizität sowie
- Datensicherheit und Datenschutz

von elektronischen Daten aller Art über lange Aufbewahrungszeiträume hinweg zu genügen. Gegenstand und Ziel der TR ist die Beweiswerterhaltung von kryptographisch signierten Dokumenten. Konkret enthält sie einen Katalog von verpflichtenden Muss-, von empfohlenen Soll- und von optionalen Kann-Anforderungen im Hinblick auf alle Elemente und Bereiche, in denen Gestaltungsbedarf hinsichtlich einer vertrauenswürdigen Langzeitspeicherung besteht. Die TR ist auf der Internetseite des BSI veröffentlicht.

Die Archivlösung der SV-Träger kann gegen die in der TR-ESOR aufgeführten Anforderungen geprüft und deren Konformität festgestellt werden. Dies erfolgt über vom BSI zertifizierte Bestätigungsstellen.

Bei dieser Prüfung werden alle **Muss-Anforderungen** auf ihre uneingeschränkte Umsetzung hin überprüft. Eine Abweichung von den Muss-Anforderungen ist nicht zulässig. Die Nichteinhal-

tung von **Soll-Anforderungen** muss durch den Antragsteller schlüssig und nachvollziehbar, schriftlich begründet werden.

Die Prüfdienste des Bundes und der Länder haben einige Inhalte der TR-ESOR im Anhang 1 zum Leitfaden dargestellt. Die Texte in der Spalte „Anforderungen“ sind aus dem Hauptdokument der TR-ESOR übernommen worden. Es sind nur die Anforderungen aufgeführt, die aufgrund entsprechender rechtlicher Vorgaben für SV-Träger von denen der TR-ESOR abweichen. Die sonstigen Grundanforderungen sind der TR-ESOR selbst zu entnehmen.

Es wird empfohlen, die im TR-ESOR-Hauptdokument und seiner Anlage B (Profilierung für Bundesbehörden) enthaltenen **Muss- und Soll-Anforderungen** hinsichtlich einer revisionssicheren Langzeitspeicherung elektronischer Dokumente zu beachten und umzusetzen. Die Empfehlung gilt auch für die Langzeitspeicherung nicht signierter Dokumente / Daten.
Die Prüfdienste des Bundes und der Länder werden die in der Anlage aufgeführten Muss- und Soll-Anforderungen bei Prüfungen der revisionssicheren Langzeitspeicherung als Prüf- und Bewertungsgrundlage heranziehen.

7.4 Löschung von Daten der elektronischen Kommunikation

Die Verpflichtung zur Löschung personenbezogener Daten ergibt sich aus Art. 17 Abs. 1 DS-GVO. Die Einhaltung dieser Verpflichtung kann ab einem gewissen Komplexitätsgrad nur durch ein detailliertes Löschkonzept[63] gewährleistet werden. Zudem müssen in einem Verfahrensverzeichnis gem. Art. 30 Abs. 1 Buchstabe f DS-GVO Löschfristen spezifiziert werden.

Bei der Erstellung des Löschkonzeptes und der Löschfristen ist zu beachten, dass hierunter nicht nur Nutzdaten sondern auch Metadaten (z. B. Log-Daten zu Web-Seiten, Tracking-Daten und App-Daten) fallen.

Es wird empfohlen, die speziell für den Bereich der Online-Kommunikation geltenden Löschregeln in das Gesamtkonzept des SV-Trägers zur Löschung von Daten aufzunehmen.

[63] Vorgaben zur Erstellung und den Inhalten eines Löschkonzeptes enthält die DIN 66398 („Leitlinie Löschkonzept“).

Anhang 1 Auszug BSI Technische Richtlinie 03125 „Beweiswerterhaltung kryptographisch signierter Dokumente“

(Version 1.2.1 vom 15.03.2018)

Abschnitt aus TR-ESOR	Thema:	Anforderungen:	Fundstelle:
4.2.1.2	Neusignierung	Gem. **§ 15 VDG** sind qualifiziert digital signierte oder zeitgestempelte Daten „*durch geeigneten Maßnahmen neu zu schützen, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird*“ , wenn sie für längere Zeit in kryptographisch signierter Form benötigt werden, als der Signatur-, Siegel- bzw. Zeitstempelalgorithmus als geeignet (technisch sicher) beurteilt werden kann. Da auch Validierungsdaten elektronische Signaturen bzw. Siegel bzw. Zeitstempel enthalten, unterliegen sie ebenso dem Erfordernis der Maßnahmen zur langfristigen Beweiswerterhaltung. Erst durch ihre Einbeziehung in diese Maßnahmen kann die Unversehrtheit und damit Echtheit eines Zertifikats, einer Gültigkeitsabfrage oder eines Zeitstempels langfristig überprüft werden. § 15 des Vertrauensdienstegesetz begründet allerdings keine Rechtspflichten. Der Zweck dieser technischen Vorschrift ist darauf beschränkt, ein geeignetes Verfahren für eine langfristige Beweiswerterhaltung zu beschreiben. Der qualifizierte Vertrauensdiensteanbieter hat jedoch den Signatur-Unterzeichner bzw. Siegel- bzw. Zeitstempelersteller gem. **§ 13 Abs. 1 Satz 2 VDG** darauf hinzuweisen, dass Daten mit einer qualifizierten elektronischen Signatur bzw. einem qualifizierten elektronischen Siegel bzw. mit einem qualifizierten elektronischen Zeitstempel bei Bedarf gem. § 15 VDG durch geeignete Maßnahmen neu zu schützen sind, bevor der Sicherheitswert der vorhandenen Signaturen, Siegel oder Zeitstempel durch Zeitablauf geringer wird. Die Anwendung des Verfahrens ist damit grundsätzlich als eine Obliegenheit im Umgang mit kryptographisch signierten Daten anzusehen. Auch wenn somit grundsätzlich lediglich eine Obliegenheit begründet, kann eine Rechtspflicht zur Anwendung des **§ 15 VDG** bestehen. Diese muss sich dann jedoch aus anderen Gesetzen, Normen oder aus vertraglichen Regelungen ergeben. Eine	§ 15 VDG

Abschnitt aus TR-ESOR	Thema:	Anforderungen:	Fundstelle:
		Rechtspflicht zur Anwendung besteht immer dann, wenn der Empfänger auf Grund von Gesetzen oder Verträgen verpflichtet ist, den besonderen Beweiswert qualifiziert signierter bzw. gesiegelter bzw. zeitgestempelter elektronischer Dokumente zu erhalten. Das eIDAS-Durchführungsgesetz **(eIDAS-DG)** enthält unter „Begründung, B. Besonderer Teil, Zu Teil 2 (Allgemeine Vorschriften für qualifizierte Vertrauensdienste), zu § 15 (Langfristige Beweiserhaltung)“ die folgenden weiteren Ausführungen zum Verfahren, wie und wann die langfristige Sicherung qualifiziert kryptographisch signierter Daten zu erfolgen hat: *„Die langfristige Sicherung qualifiziert signierter Daten erfolgt derzeit durch Neusignieren oder erneutes Zeitstempeln der signierten Daten, bevor die verwendeten Algorithmen und Parameter ihre Sicherheitseignung verlieren. Die Beobachtung der Sicherheitseignung und die Neusignierung bzw. das erneute Zeitstempeln ist nicht Bewahrungsdiensten vorbehalten, sondern kann auch von den genannten Personen selbst vorgenommen werden.* *Die Einhaltung des Standes der Technik wird jedenfalls dann vermutet, wenn die entsprechenden und jeweils aktuellsten, im Bundesanzeiger bekanntgemachten Schutzprofile und Technischen Richtlinien des BSI eingehalten werden. Auf die Konformität mit europäischen Standards ist zu achten.“* Dies ist die Grundlage der Beweiswerterhaltung elektronischer Dokumente.	
4.3.1	Vertrauensdiensteanbieter	Die Vergabe qualifizierter Zertifikate ist nach **eIDAS-Verordnung (Anhang I bzw. III)** qualifizierten Vertrauensdiensteanbietern vorbehalten, die mindestens die Sicherheitsanforderungen der eIDAS-Verordnung erfüllen. Gem. **Art. 34 Abs. 1 eIDAS-Verordnung** muss ein qualifizierter Bewahrungsdienst für qualifizierte elektronische Signaturen von einem qualifizierten Vertrauensdiensteanbietern gem. **Art. 3 Nr. 17 eIDAS-Verordnung** erbracht werden.	Art. 3, 34 eIDAS-Verordnung

Abschnitt aus TR-ESOR	Thema:	Anforderungen:	Fundstelle:
		Für die langfristige Sicherung und Überprüfbarkeit der Authentizität und Integrität kryptographisch signierter Daten und Dokumente folgt daraus: Die Erstellung und Prüfung qualifizierter elektronischer Signaturen, Siegel bzw. Zeitstempel für aufbewahrte kryptographisch signierte elektronische Daten und Dokumente sollen gem. der eIDAS-Verordnung und des Vertrauensdienstegesetzes erfolgen.	
4.3.1	Integritätssicherung nicht signierter Daten	Die Integrität nicht signierter, gesiegelter bzw. zeitgestempelter Daten kann zusätzlich ab dem Zeitpunkt der Überführung in einen ECM[64] / Langzeitspeicher automatisch durch geeignete kryptographische Sicherungsmittel wie elektronische Archiv(eingangs)hashwerte oder -signaturen bzw. -siegel oder (qualifizierte) Archiv(eingangs)zeitstempel gesichert werden. *Handelt es sich um rechtlich bedeutsame Dokumente bzw. erfordert die Art der Daten eine revisionssichere Archivierung, so **müssen** diese mit einer QES versehen im Langzeitspeicher abgelegt werden.*	§§ 110a ff. SGB IV
5	**Funktionen einer Middleware zum Beweiswerterhalt**		
5.1.1	**Archivierung signierter und unsignierter Daten**		

[64] ECM = Enterprise Content Management

Abschnitt aus TR-ESOR	Thema:	Anforderungen:	Fundstelle:
(A5.1-4)	Konformitätsprüfung der Datenformate	Die Middleware **muss**[65] vor der Ablage im ECM/Langzeitspeicher die Syntax der zur Aufbewahrung übergebenen Archivdatenobjekte auf Konformität mit den für die Archivierung durch die Nutzer und Betreiber eines Archivsystems definierten und spezifizierten Datenformaten prüfen. Bei Nichtübereinstimmung muss dann die Ablage im ECM/Langzeitspeicher abgelehnt werden.	
5.2	**Organisatorische Anforderungen**	Die organisatorischen Anforderungen legen die nicht-technischen Bedingungen fest, die vorzugsweise bereits vor oder bei der Einführung einer Middleware für den Beweiswerterhalt geschaffen werden müssen. Dieses Kapitel versteht sich als Hinweis an die Benutzer einer solchen Middleware und legt keine formalen Kriterien fest.[66]	
6	**Abgeleitete technische Anforderungen**	Der folgende Abschnitt beschreibt abgeleitete und vornehmlich technische Anforderungen, die bei der Einrichtung und dem Betrieb einer zu dieser Richtlinie konformen Middleware zum Beweiswerterhalt zu erfüllen sind.	
(A6.1-3)	Getrennte Mandantenverwaltung	Die TR-ESOR-Middleware ***muss***[67] in der Lage sein, getrennte Mandanten zu verwalten. Dies bedeutet insbesondere eine strikte (logische) Separierung der im ECM/Langzeitspeicher abgelegten Archivdatenobjekte aber auch eine Trennung der für den Beweiswerterhalt relevanten Daten (Hashbäume).	

[65] Muss-Anforderung entsprechend Anlage TR-ESOR-B: Profilierung für Bundesbehörden (Version 1.2.1 vom 15.03.2018).

[66] Abweichend zur TR-ESOR können im Bereich der SV-Träger formale Anforderungen Muss-Kriterien sein.

[67] Bei IT-Dienstleistern/RZ, die für mehrere SV-Träger tätig sind, **muss** eine entsprechende Trennung der Daten erfolgen!

Abschnitt aus TR-ESOR	Thema:	Anforderungen:	Fundstelle:
(A6.2-1)	Plattform- und herstellerunabhängige Datenformate	Im Interesse der dauerhaften Verfügbarkeit und Verkehrsfähigkeit der zu archivierenden Dokumente und Daten **müssen**[68] ausschließlich Datenformate eingesetzt werden, die eine plattform- und herstellerunabhängige Archivierung in langfristig verkehrsfähiger Form ermöglichen. Kapitel 4 von TR-ESOR-F führt im Detail die empfohlenen Formate auf.	
6.4	**IT-Infrastruktur**	Die nachfolgend genannten technischen Sicherungsmaßnahmen für die TR-ESOR-Middleware und für das gesamte Archivsystem dienen dem Beweiswerterhalt und umfassen physische Sicherungsmaßnahmen, logische Zugriffskontrollen sowie Datensicherungs- und Auslagerungsverfahren für den Regel- und den Notbetrieb. Dieses Kapitel versteht sich als Hinweis an die Benutzer/Betreiber einer solchen Middleware und legt keine formalen Kriterien fest.[69] Der ECM/Langzeitspeicher stellt die Datensenke des elektronischen Archivs dar. Die archivierten Daten und Dokumente sind hier sicher gespeichert, inklusive aller für die langfristige Aufbewahrung und Verfügbarkeit nötigen Verkehrs- und Verwaltungsinformationen.	

[68] Änderung als Muss-Anforderung entsprechend Anlage TR-ESOR-B: Profilierung für Bundesbehörden (Version 1.2.1 vom 15.03.2018).

[69] Abweichend zur TR-ESOR können im Bereich der SV-Träger formale Anforderungen Muss-Kriterien sein.

Abschnitt aus TR-ESOR	Thema:	Anforderungen:	Fundstelle:
6.5	**IT-Anwendungen beim Einsatz von Archivierungsverfahren**	Neben Anforderungen an die IT-Infrastruktur und natürlich der TR-ESOR-Middleware **müssen** auch diverse Anforderungen an die vorgelagerten Fachanwendungen gestellt werden. Dieses Kapitel versteht sich als Empfehlung an die Benutzer/Betreiber einer solchen Middleware und legt keine formalen Kriterien fest.[70] Bei den zur Archivierung eingesetzten IT-Anwendungen handelt es sich im Regelfall um Softwaresysteme, die an die organisationsspezifischen Besonderheiten und Archivierungsanforderungen anzupassen sind. Eine Anwendung im Sinn dieser Richtlinie kann aus mehreren Einzelkomponenten oder Programmen bestehen. Es ist nicht notwendigerweise ein monolithisches Programm oder ein einzelnes System. In den vorgelagerten Anwendungssystemen werden die später zu archivierenden Dokumente und Daten erzeugt und bearbeitet. Bis zum Zeitpunkt der Archivierung werden sie dabei auf den zu diesen Anwendungssystemen gehörenden Datenspeichern vorgehalten.	
6.5	Trusted Viewer	Für die Anzeige von qualifiziert signierten elektronischen Daten und Dokumenten ***muss***[71] die Anwendung oder die Anwendungsumgebung eine vertrauenswürdige Anzeigekomponente (Trusted Viewer) zur Verfügung stellen.	
8	**IT-Sicherheitskonzept**		

[70] Abweichend zur TR-ESOR können im Bereich der SV-Träger formale Anforderungen Muss-Kriterien sein.

[71] SV-Träger muss in der Lage sein, die Signatur von Dokumenten/Daten zu überprüfen.

Abschnitt aus TR-ESOR	Thema:	Anforderungen:	Fundstelle:
8.2	**Maßnahmen**	Um die oben angegebenen Sicherheitsziele für die Middleware und den ECM/Langzeitspeicher in der Ausprägung der empfohlenen Referenzarchitektur zu erfüllen, sind die folgenden Maßnahmen erforderlich. Dieses Kapitel versteht sich als Hinweis an die Benutzer einer solchen Middleware bzw. eines ECM / Langzeitspeichers und legt keine formalen Kriterien fest.[72] Hinweis: Es ist zu beachten, dass dieser generische Maßnahmenkatalog auf keinen Fall ein konkretes Sicherheitskonzept (gem. bspw. den IT-Grundschutz-Katalogen des BSI) ersetzen kann, das den lokalen und organisationsspezifischen Bedürfnissen und Gegebenheiten angepasst ist.	
8.2.1	Übergreifende Maßnahmen	Vor dem Einrichten eines elektronischen Archivsystems mit dem Fokus auf dem Beweiswerterhalt muss ein die technischen Systeme und sämtliche relevanten Prozesse abdeckendes IT-Sicherheitskonzept basierend auf einer standardisierten Methodik (z. B. als Konzept für ein Managementsystem für Informationssicherheit (ISMS) auf Basis der BSI-Standards 200-1, -2, -3. **IT-Grundschutz**) erstellt und mit der Inbetriebnahme umgesetzt werden. Das IT-Sicherheitskonzept **muss** regelmäßig (z. B. einmal pro Jahr) auf den aktuellen Stand gebracht werden. Die Maßnahmen, die sich aus dem IT-Sicherheitskonzept und dessen Überarbeitung ergeben, **müssen** - soweit wirtschaftlich vertretbar[73] - zeitnah umgesetzt werden. Dies	

[72] Abweichend zur TR-ESOR können im Bereich der SV-Träger formale Anforderungen Muss-Kriterien sein.

Abschnitt aus TR-ESOR	Thema:	Anforderungen:	Fundstelle:
		gilt insbesondere für die Definition und Umsetzung der Verantwortlichkeiten und Kompetenzen, der fachlichen Prozesse sowie sicherer Administrations- und Kontrollprozesse. Insbesondere für Einrichtungen, Organisationen und Unternehmen der öffentlichen Verwaltung **soll** das Einrichten und der Betrieb eines Archivsystems mit einer Middleware zum Beweiswerterhalt einem IT-Grundschutz-Audit mit dem Ziel der Zertifizierung unterzogen werden, um auch die jeweiligen Prozesse und Organisationen in der Einsatzumgebung nachweislich zielgerichtet definiert zu haben.	

[73] Wirtschaftliche Aspekte sind nachrangig, wenn rechtliche Vorgaben (z. B. der „UP Bund“) eine zeitnahe Umsetzung fordern.